DIOPHANTINE EQUATIONS

Gaurish Korpal[1]
gaurish.korpal@niser.ac.in

Summer Internship Project Report

---

[1] 1st year Int. MSc. Student, National Institute of Science Education and Research, Bhubaneswar (Odisha)

Certificate

Certified that the summer internship project report "Diophantine Equations" is the bonafide work of "Gaurish Korpal", 1st Year Int. MSc. student at National Institute of Science Education and Research, Bhubaneswar (Odisha), carried out under my supervision during May 18, 2015 to June 16, 2015.

Place: Pune
Date: June 16, 2015

Prof. S. A. Katre
Supervisor
Professor & Head,
Department of Mathematics,
Savitribai Phule Pune University,
Pune 411 007, Maharashtra

Acting Director (Hon.),
Bhaskaracharaya Pratishthana,
Pune 411 004, Maharashtra

Abstract

The solution in integers of algebraic equations in more than one unknown with integral coefficients is one of the most difficult problem in the theory of numbers. The most eminent mathematicians like Diophantus (3^{rd} century), Brahmagupta (7^{th} century), Bhaskaracharya (12^{th} century), Fermat (17^{th} century), Euler (18^{th} century), Lagrange (18^{th} century) and many others devoted much attention to these problems. The efforts of many generations of eminent mathematicians notwithstanding, this branch of theory of numbers lacks mathematical methods of generality. So, I have tried to list out some basic tactics, and prove elementary theorems which we can encounter while dealing with diophantine equations. The study of diophantine equations involves an interplay among number theory, calculus, combinatorics, algebra and geometry.

Contents

Introduction

A *diopantine equation* is an expression of form:

$$f(x_1, x_2, \dots, x_n) = 0$$

where f is an $n-$variable function with $n \geq 2$.[1] If f is a polynomial with integral coefficients, then this equation is called *algebraic diophantine equation.*
If we call $\mathbb{F}$ to be the algebraic system[2] (like $\mathbb{Z}$, $\mathbb{Z}^+$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ etc.) in which we will solve our equation, then an $n-$tuple $(x_1^0, x_2^0, \dots, x_n^0) \in \mathbb{F}^n$ satisfying the equation is called a *solution* of the equation. An equation having atleast one solution is called *solvable.*

The *theory of diophantine equations* is that branch of number theory which deals with finding non-trivial solutions of polynomial equations in non-negative integers (a monoid), $\mathbb{Z}$ (a ring) or $\mathbb{Q}$ (a non-algebraically closed field).

While dealing with *Diophantine Equations* we ask the following question:

Is the equation solvable? If it is solvable, determine all of its solutions (finite or infinite).

A complete solution of equations is possible only for a limited types of equation. Also we will see that for equation of degree higher than the second in two or more unknowns the problem becomes rather complicated. Even the more simple problem of establishing whether the number of integral solutions is finite or infinite present extreme difficulties.

The theoretical importance of equations with integral coefficients is great as they are closely connected with many problems of number theory. Many puzzles involving numbers lead naturally to a quadratic Diophantine equation. So far there is not a clean theory for higher degree analogues of equations of second degree in three unknowns. Even at the specific level of quadratic diophatine equations, there are unsolved problems, and the higher degree analogues of some specific quadratic diophatine equations, particularly beyond third, do not appear to have been well studied.

There is interesting role of *Descartes' Coordinate Geometry* in solving *diophantine equations*, since it allows algebraic problems to be studied geometrically and vice versa. As in case of finding Pythagorean Triples (integer solutions of Pythagoras Theorem), finding non-trivial primitive i.e. pairwise relatively prime integer solutions of $X^2 + Y^2 = Z^2$ is equivalent to finding *rational points* on unit circle centred at origin i.e. $x^2 + y^2 = 1$ (a conic section). Similarly the problem of finding rational solutions for the diophantine equation: $y^2 = x^3 + c$, $c \in \mathbb{Z} \setminus \{0\}$, can be solved using Bachet's *duplication formula* (rather complicated) which can be derived easily using *geometry.* Bachet's complicated algebraic formula has a simple geometric interpretation in terms of intersection of a tangent line with an elliptic curve (a cubic curve).

While discussing Unique Factorization Domains we will review ring theory. Also, in order to prove a special case of Mordell's Theorem we will define a geometric operation which will take the set of rational solutions to cubic equation and turn it into abelian group. Thus we will also have to deal with algebra!

In Chapter - 1, I have tried to present some tactics which we can follow to handle diophantine equations. Then in Chapter - 2, I will discuss some of the well studied types of diophantine equations.

I believe that the reader will find this report interesting since I have tried to deal, in details, with number of aspects of dioiphantine equations, right from modular arithmetic to elliptic curves.

---

[1] Equations in one variable are *very* easy to solve in integers. If we denote n^{th} degree equation as: $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \quad (n \geq 1)$ then only divisors of a_0 *can* be integral root of our equation. For proof see [7] or [10]

[2] In Russian- speaking countries *algebraic systems* are called *algebraic structures*, see [18].

Chapter 1

Tools to Deal with Diophantine Equations

Here I will describe the general tools one can use to approach a diophantine equation. This idea of classification of methods have been taken from [5] and [17].

1.1 Modular Arithmetic & Parity

This is one of the most useful technique. Simple modular arithmetic considerations (like parity) help to drastically reduce the range of the possible solutions. This technique is most successful in proving a given diophantine equation is not solvable.[1] Consider the following example:

Example 1.1.1. *Find all rational solutions of* $x^2 + y^2 = 3$ *.*

Solution. Since x and y are rational numbers we can write them as: $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, such that $X, Y, Z \in \mathbb{Z}$, $Z \neq 0$ and $gcd(X, Y, Z) = 1$. Thus we can restate given problem as:

Find all non-zero integer solutions of $X^2 + Y^2 = 3Z^2$*, such that* $gcd(X, Y, Z) = 1$*.*

We know that any perfect square leaves a residue of 1 or 0 modulo 3. Let(X_0, Y_0, Z_0) be a solution to this equation such that $gcd(X_0, Y_0, Z_0) = 1$. Thus in modulo 3:

$$\begin{gathered}
\Rightarrow X_0^2 + Y_0^2 \equiv 3Z_0^2 \pmod 3 \\
\Rightarrow X_0^2 + Y_0^2 \equiv 0 \pmod 3 \\
\Rightarrow X_0^2 \equiv 0 \pmod 3 \qquad \& \qquad Y_0^2 \equiv 0 \pmod 3 \\
\Rightarrow X_0 \equiv 0 \pmod 3 \qquad \& \qquad Y_0 \equiv 0 \pmod 3 \qquad (1.1) \\
\Rightarrow X_0^2 \equiv 0 \pmod 9 \qquad \& \qquad Y_0^2 \equiv 0 \pmod 9 \\
\Rightarrow X_0^2 + Y_0^2 \equiv 0 \pmod 9 \\
\Rightarrow 3Z_0^2 \equiv 0 \pmod 9 \\
\Rightarrow Z_0^2 \equiv 0 \pmod 3 \\
\Rightarrow Z_0 \equiv 0 \pmod 3 \qquad (1.2)
\end{gathered}$$

From (1.1) and (1.2) we get $\gcd(X_0, Y_0, Z_0) = 3$. Contradiction to our assumption that $gcd(X_0, Y_0, Z_0) = 1$. Hence the given equation has no solution in rational numbers.

Remark: Similarly you can prove that $x^3 + 2y^3 + 4z^3 = 9w^3$ has no non-trivial solution, since perfect cubes are $\equiv 0, \pm 1 \pmod 9$

Example 1.1.2. *Show that the equation*

$$\sum_{t=1}^{99} (x + t)^2 = y^z$$

is not solvable in integers x,y,z, with $z > 1$*.*

Solution. Simplify LHS and check for residues in appropriate modulo. Important point to note is that $z \geq 2$.

---

[1] For more examples refer Chapter - 2 of [5]

1.2 Inequalities

Sometimes we are able to restrict the intervals in which we should search for solutions by using appropriate inequalities.

Example 1.2.1. *Find all integer solutions of* $x^3 + y^3 = (x + y)^2$

Solution. The given equation is equivalent to:

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

Now since RHS and LHS are positive we get following inequalities:

$$(x - 1)^2 \leq 1, \qquad (y - 1)^2 \leq 1$$

Thus $x, y \in [0, 2]$. Hence the solutions are $(0, 1), (1, 0), (1, 2), (2, 1), (2, 2)$

Example 1.2.2. *Find all positive integers* $n, k_1, k_2, \ldots, k_n$ *such that*

$$\sum_{i=1}^{n} k_i = 5n - 4 \quad \textit{and} \quad \sum_{i=1}^{n} \frac{1}{k_i} = 1$$

(Putnam Mathematical Competition)

Solution. By the arithmetic-harmonic mean(AM-HM) inequality

$$(k_1 + k_2 \ldots + k_n)\left(\frac{1}{k_1} + \frac{1}{k_2} + \ldots + \frac{1}{k_n}\right) \geq n^2$$

We must thus have $5n - 4 \geq n^2$, so $n \leq 4$. Without loss of generality, we may suppose that $k_1 \leq \ldots \leq k_n$

If $n = 1$, we must have $k_1 = 1$, and hereinafter we cannot have $k_1 = 1$.

If $n = 2$, then $(k_1, k_2) \in \{(2, 4), (3, 3)\}$, neither of which works.

If $n = 3$, then $k_1+k_2+k_3 = 11$, so $2 \leq k_1 \leq 3$. Hence $(k_1, k_2, k_3) \in \{(2, 2, 7), (2, 3, 6), (2, 4, 5), (3, 3, 5), (3, 4, 4)\}$, and only $(2, 3, 6)$ works.

If $n = 4$, we must have equality in the AM-HM inequality, which happens only when $k_1 = k_2 = k_3 = k_4 = 4$.

Hence the solutions are:

$$\begin{cases} n = 1 & \text{and} \quad k_1 = 1, \\ n = 3 & \text{and} \quad (k_1, k_2, k_3) \quad \text{is a permutation of} \quad (2, 3, 6), \\ n = 4 & \text{and} \quad (k_1, k_2, k_3, k_4) = (4, 4, 4, 4). \end{cases}$$

1.3 Parametrization

If given diophantine equation has infinite number of solutions then we can represent given diophantine equation in parametric form as:

$$\begin{cases} x_1 = g_1(k_1, k_2, \ldots, k_{t_1}), \\ x_2 = g_2(k_1, k_2, \ldots, k_{t_2}) \\ \vdots \\ x_n = g_n(k_1, k_2, \ldots, k_{t_n}) \end{cases}$$

where $k_i \in \mathbb{F}$ [i.e. the algebraic system in which we are searching for solution]

Example 1.3.1. *Find all positive integral solutions of:*

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

if the numbers x,y,z are pairwise relatively prime.
(A. O. Gelfond)

Solution. Note that if the triplet x, y, z is a solution of given equation and the numbers x, y and z possess no common divisors (except, of course, unity), then they are pairwise relatively prime. Indeed, let x and y be multiples of a prime number p ($p > 2$).Then from equality

$$\left(\frac{x}{p}\right)^2 + 2\left(\frac{y}{p}\right)^2 = \left(\frac{z}{p}\right)^2$$

with an integral left-hand side it follows that z is a multiple of p. The same conclusion holds if x and z, or y and z are multiples of p.

Notice that x must be an odd number for the $gcd(x, y, z) = 1$. For if x is even, then the left-hand side (LHS) of given equation is an even number so that z is also even. But then x^2 and z^2 are multiples of 4. From this it follows that $2y^2$ is divisible by 4, in other words that y must also be an even number. Thus, if x is even then all three numbers x, y, z must be even. Thus, in a solution not having a common divisor different from unity x must be odd. From this it immediately follows that z must also be odd. Transferring x^2 into the right-hand side (RHS) of given equation equation we get

$$2y^2 = z^2 - x^2 = (z + x)(z - x) \tag{1.3}$$

But $(z + x)$ and $(z - x)$ have the greatest common divisor 2. Let their greatest common divisor be d. Then

$$z + x = kd, \qquad z - x = ld$$

where k and l are integers. Adding together these equalities, then subtracting the second one from the first we arrive at

$$2z = d(k + l), \quad 2x = d(k - l)$$

But z and x are odd and relatively prime. Therefore the greatest common divisor of $2x$ and $2z$ must be equal to 2, that is d = 2.

Thus, either $\frac{z+x}{2}$ or $\frac{z-x}{2}$ is odd. Therefore either $z + x$ and $\frac{z-x}{2}$ are relatively prime or $z - x$ and $\frac{z+x}{2}$ are relatively prime.

In the first case (1.3) leads to:

$$\begin{cases} z + x = n^2, \\ z - x = 2m^2 \end{cases}$$

while in second case (1.3) leads to:

$$\begin{cases} z + x = 2m^2, \\ z - x = n^2 \end{cases}$$

where n and m are positive integers and m is odd.
Solving these two systems of equations we get:

$$\begin{cases} x = \frac{n^2-2m^2}{2}, \\ y = mn \\ z = \frac{n^2+2m^2}{2} \end{cases} \quad or \quad \begin{cases} x = \frac{2m^2-n^2}{2}, \\ y = mn \\ z = \frac{n^2+2m^2}{2} \end{cases}$$

respectively, where m is odd.
Now combine above two expressions and replace $n = a$ and $m = 2b + 1$ where $a, b \in \mathbb{Z}^+$ to get general parametric form as:

$$\begin{cases} x = \pm\frac{a^2-8b^2-8b-2}{2}, \\ y = a(2b + 1) \\ z = \frac{a^2+8b^2+8b+2}{2} \end{cases}$$

Remark: Notice that we also used *parity* technique to reduce the number of cases to two only.

Example 1.3.2. *Prove that equation:*

$$x^2 = y^3 + z^5$$

has infinite number of solutions in positive integers.

Solution. Observe that if $n \in \mathbb{Z}^+$ is our parameter and since there is sum on RHS, there should be a power of $(n+1)$, thus x, y, z should look like:

$$\begin{cases} x = n^{\alpha}(n+1)^a, \\ y = n^{\beta}(n+1)^b \\ z = n^{\gamma}(n+1)^c \end{cases}$$

Now degree of $(n+1)$ (in initial state), in RHS (i.e. y, z) should be one less than that in LHS (i.e. x). Also since gcd(3,5)=1 we get $lcm(3,5) = 3 \times 5 = 15$ and $15 + 1 = 2 \times 8$ so, we can set $a = 8, b = 5, c = 3$ thus:

$$\Rightarrow n^{2\alpha}(n+1)^{16} = n^{3\beta}(n+1)^{15} + n^{5\gamma}(n+1)^{15}$$

$$\Rightarrow n^{2\alpha}(n+1) = n^{3\beta} + n^{5\gamma}$$

Now equating exponents we get following linear diophantine equations:

$$\begin{cases} 2\alpha + 1 = 3\beta \\ 2\alpha = 5\gamma \end{cases} \quad \text{or} \quad \begin{cases} 2\alpha + 1 = 5\gamma \\ 2\alpha = 3\beta \end{cases}$$

we get a solution:

$$\begin{cases} \alpha = 10 \\ \beta = 7 \\ \gamma = 4 \end{cases} \quad \text{or} \quad \begin{cases} \alpha = 12 \\ \beta = 8 \\ \gamma = 5 \end{cases}$$

Finally we get our solutions for all $n \in \mathbb{Z}^+$ as:

$$\begin{cases} x = n^{10}(n+1)^8, \\ y = n^7(n+1)^5 \\ z = n^4(n+1)^3 \end{cases} \quad \text{or} \quad \begin{cases} x = n^{12}(n+1)^8, \\ y = n^8(n+1)^5 \\ z = n^5(n+1)^3 \end{cases}$$

1.4 Method of Infinite Descent

Let P be a property concerning non-negative integers and let $\{P(n)\}_{n \geq 1}$ be the sequence of propositions, then:

$$P(n) \quad : \quad n \text{ satisfies property } P$$

Then following methods can be used to prove that proposition $P(n)$ is *false* for all large enough n:

1. **Method of Finite Descent**
   Let k be a non-negative integer, suppose that:

   - $P(k)$ is not true;
   - whenever $P(m)$ is true for a positive integer $m > k$, then there must be some smaller j, $m > j > k$ for which $P(j)$ is true

   Then $P(n)$ is false for all $n \geq k$
   Remark: This method is just contrapositive of *Principle of Mathematical Induction* (strong form).

2. **Method of Infinite Descent**
   Let k be a non-negative integer, suppose that:

   - whenever $P(m)$ is true for a positive integer $m > k$, then there must be some smaller j, $m > j > k$ for which $P(j)$ is true

   Then $P(n)$ is false for all $n > k$
   Remark: *Bhaskaracharya* extended *Brahmagupta's* work on equations of form $x^2 - Dy^2 = A$ (where D is not a perfect square), by describing this method of infinite descent and called his method *chakravala*.

The *method of infinite descent* implies following two statements which we will use for solving diophantine equations:

MID1 There is no infinite decreasing sequence of non-negative integers

MID2 If n_0 is the smallest positive integer n for which $P(n)$ is true, then $P(n)$ is false for all $n < n_0$.

MID3 If the sequence of non–negative integers $(n_i)_{i\geq 1}$ satisfies the inequalities $n_1 \geq n_2 \geq \ldots$, then there exists i_0 such that $n_{i_0} = n_{i_0+1} = \ldots$.

We apply this method when we have found a solution of given diophantine equation and want to prove that this is the only solution of given equation.

Example 1.4.1. *Solve in non-negative integers the equation:*

$$x^3 + 2y^3 = 4z^3$$

Solution. We can observe that $(0, 0, , 0)$ is a solution of given equation. Now let's check whether this is only solution. Let's try to validate MID1 for this case.

Let (x_1, x_2, x_3) be the non-trivial solutions,

$$\Rightarrow x_1^3 + 2y_1^3 = 4z_1^3$$

Now we will apply *parity* argument. Since RHS is even, LHS should also be even, thus x_1^3 is even. This implies that $2|x_1$, thus $x_1 = 2x_2$ for some $x_1 > x_2$.
Now substitute this in above equation to get:

$$\Rightarrow 4x_2^3 + y_1^3 = 2z_1^3$$

Now again by *parity* argument, $y_1 = 2y_2$ for some $y_1 > y_2$.
Now substitute this in above equation to get:

$$\Rightarrow 2x_2^3 + 4y_2^3 = z_1^3$$

Now again by *parity* argument, $z_1 = 2z_2$ for some $z_1 > z_2$.
Now substitute this in above equation to get:

$$\Rightarrow x_2^3 + 2y_2^3 = 4z_2^3$$

Thus we have generated a new solution (x_2, y_2, z_2) which is smaller than earlier solution. Hence by repeating above method we can generate infinite decreasing sequence $x_1 > x_2 > \ldots$ such that $(x_n, y_n, z_n)_{n\geq 1}$ is a solution of given equation.
But x_n is a non-negative integer. Thus this contradicts MID1. Thus $(0, 0, 0)$ is only non-negative solution of the given equation.

Example 1.4.2. *Find all pairs of positive integers* (a, b) *such that* $ab + a + b$ *divides* $a^2 + b^2 + 1$ *(Mathematics Magazine)*

Solution. The divisibility condition can be written as following diophantine equation

$$k(a + b + ab) = a^2 + b^2 + 1$$

for some positive integer k. Then by *trial and error method* we find that permutations of $(a, b) = (1, 1)$, $(1, 4), (4, 9), (9, 16)$ satisfy this diophantine equation. Based on this we conjecture that : either $a = b = 1$ or a and b are consecutive squares are "only" possible solutions.

If $k = 1$, then our diophantine equation is equivalent to:

$$(a - b)^2 + (a - 1)^2 + (b - 1)^2 = 0,$$

from which by *suitable inequalities* we get $a = b = 1$.

If $k = 2$, then our diophantine equation can be written as

$$4a = (b - a - 1)^2$$

forcing a to be a square, say $a = d^2$. Then $b - d^2 - 1 = \pm 2d$, so $b = (d \pm 1)^2$, and a and b are consecutive squares.

Thus we have proved that our conjecture is half true. Now what remains to prove is that these are the "only" solutions.

Now assume that there is a solution with $k \geq 3$, and let (a, b) be the solution with a being "minimal" and $a \leq b$. Write our diophantine equation as a quadratic in b:

$$b^2 - k(a+1)b + (a^2 - ka + 1) = 0.$$

Because one root, b, is an integer, the other root, call it r, is also an integer.
Since our diophantine equation must be true with r in place of b, we conclude that $r > 0$. Because $a \leq b$ and the product of the roots, $a^2 - ka + 1 < a^2$, we must have $r < a$. But then (r, a) is also a solution to given diophantine equation, contradicting the minimality of a. Hence for $k \geq 3$ there is no solution for our diophantine equation.
Thus our conjecture was true and for either $a = b = 1$ or a and b being consecutive squares provide all pairs of positive integers (a, b) such that $ab + a + b$ divides $a^2 + b^2 + 1$.

Remark: The most important application of method of infinite descent is to bring a contradiction about minimality of our selected solution thus leading to non-existence of all those "conjectured solutions". More application of this method will be seen in Section 2.4

1.5 Quadratic Reciprocity

Let's firstly review certain definitions:

Definition 1.5.1 (Quadratic residue and non-residue modulo p)**.** Consider a algebraic congruence of form:

$$x^k \equiv c \pmod{p}$$

where p is a prime number and $k \in \mathbb{Z}^+$, to be solved for x. For a given number c (not zero modulo p),then:

- If this equation is solvable, then c is called a k^{th} power *residue* to modulus p
- If this equation is not solvable, then c is called a k^{th} power *non-residue* to modulus p

For $k = 2$, we get *quadratic residues* and *quadratic non-residues* modulo p.
ILLUSTRATION: For $p = 13$, we get $\{1, 3, 4, 9, 10, 12\}$ as *quadratic residues* and remaining residues, $\{2, 5, 6, 7, 8, 11\}$, as *quadratic non-residues* modulo 13.

Definition 1.5.2 (Order of a modulo p)**.** If $\gcd(a, p) = 1$, then we define *order*[2] of a modulo p as the smallest exponent $e \geq 1$ for which $a^e \equiv 1 \pmod{p}$. It is denoted by $e_p(a)$.
ILLUSTRATION: Order of 2 modulo 7 is 3, thus $e_7(2) = 3$.

Definition 1.5.3 (Primitive root modulo p)**.** For given prime p, a number g with $e_p(g) = p - 1$, is called *primitive root* modulo p.
ILLUSTRATION: Since, $e_7(3) = e_7(5) = 6$, thus $g = 3, 5$ are primitive roots modulo 7 .

Definition 1.5.4 (Index of b modulo p)**.** If g is primitive root modulo prime p, then $m \in \{1, 2, \ldots, p-2, p-1\}$ is called *index*[3] of b modulo p if $b \equiv g^m \pmod{p}$. It is denoted by $I_p^g(b)$.
ILLUSTRATION: 2 is primitive root modulo 19, and $13 \equiv 32 \equiv 2^5 \pmod{19}$, thus index of 13 modulo 19 with respect to primitive root 2 is 5 or $I_{19}^2(13) = 5$.

---

[2] Note that as per *Fermat's Little Theorem* $(p-1)$ is the maximum possible order of a modulo p.

[3] Indices satisfy usual *laws of exponents* like

- $I_p^g(ab) \equiv I_p^g(a) + I_p^g(b) \mod (p-1)$
- $I_p^g(ka) \equiv kI_p^g(a) \mod (p-1)$

Definition 1.5.5 (Legendre symbol)**.** If p is a prime number, then we can write quadratic character[4] of $x^2 \equiv a \pmod{p}$, in a form called as *Legendre Symbol*, defined as[5]

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

Also note that, as per this definition,

$$a \equiv b \pmod{p} \quad \Rightarrow \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

Now let's will prove some elementary theorems which we will be using to tackle diophantine equations.

Theorem 1.5.1 (Euler's Criterion)**.** *Let p be an odd prime. Then:*

$$a^{\frac{(p-1)}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

Proof. Let g be a primitive root modulo p. Then any number[6] not congruent to $0 \pmod{p}$ is congruent to some power of g, and we know that a is a quadratic residue precisely when it is congruent to even power of g (which is one of the numbers in the series $g, g^2, g^3, \ldots, g^{p-1}$.) Now following cases are possible:

Case 1: a is a quadratic residue

$$\Rightarrow \left(\frac{a}{p}\right) = 1$$

Also it means that a is congruent to an even power of g, then for some $k \in \mathbb{Z}^+$,

$$\Rightarrow a \equiv g^{2k} \pmod{p}$$

Since a, g are not a multiple of p and $\frac{p-1}{2}$ is an integer, we can raise power $\frac{p-1}{2}$ on both sides:

$$\Rightarrow a^{\frac{p-1}{2}} \equiv g^{(p-1)k} \pmod{p}$$

Since g is the primitive root modulo p, $g^{p-1} \equiv 1 \pmod{p}$, thus:

$$\Rightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Which is equivalent to stating:

$$\Rightarrow a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

Case 2: a is a quadratic non-residue

$$\Rightarrow \left(\frac{a}{p}\right) = -1$$

Also it means that a is congruent to an odd power of g, then for some $k \in \mathbb{Z}^+$,

$$\Rightarrow a \equiv g^{2k+1} \pmod{p}$$

Since a, g are not a multiple of p and $\frac{p-1}{2}$ is an integer, we can raise power $\frac{p-1}{2}$ on both sides:

$$\Rightarrow a^{\frac{p-1}{2}} \equiv g^{(p-1)k + \frac{p-1}{2}} \pmod{p}$$

---

[4] Property of being quadratic residue or quadratic non-residue

[5] Since the quadratic residues are the numbers with even indices and the quadratic non-residues are the numbers with odd indices we can write (for proof see [15]) :

$$\left(\frac{a}{p}\right) = (-1)^{\alpha} \quad \text{where } \alpha \text{ is index of } a \text{ modulo } p \text{ for some primitive root } g$$

[6] The numbers $g, g^2, g^3, \ldots, g^{p-1}$ are all in-congruent, since g^{p-1} is the first power of g which is congruent to 1. Also none of these numbers is $\equiv 0$. Hence they must be congruent to the numbers $1, 2, \ldots, p-1$ in some order.

Since g is the primitive root modulo p, $g^{p-1} \equiv 1 \pmod{p}$, thus:

$$\Rightarrow a^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \pmod{p}$$

Now, observe that:

$$g^{\frac{p-1}{2}} \equiv k \pmod{p} \quad \Rightarrow g^{p-1} \equiv k^2 \pmod{p} \quad \Rightarrow k = \pm 1 \tag{1.4}$$

But since index is $(p-1)$, no power of g lesser than $(p-1)$ can be congruent to 1, hence, $k = -1$, thus:

$$\Rightarrow a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Which is equivalent to stating:

$$\Rightarrow a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

Finally combining both cases we prove the statement. □

Theorem 1.5.2 (Quadratic Residue Multiplication Rule)**.** *Let p be an odd prime. Then:*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

Remark: Basically this is inheritance of exponential law by indices.

Proof. From Euler's Criterion:

$$(ab)^{\frac{(p-1)}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}$$

Also,

$$(ab)^{\frac{(p-1)}{2}} = a^{\frac{(p-1)}{2}} b^{\frac{(p-1)}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$$

Combining both we get (since Left Hand Side is same in both) :

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

□

Theorem 1.5.3. *Let p be an odd prime, then:*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

Proof. As per Euler's Criterion:

$$(-1)^{\frac{(p-1)}{2}} \equiv \left(\frac{-1}{p}\right) \pmod{p}$$

Now consider both cases:

Case 1: $p = 4k + 1, k \in \mathbb{Z}^+$

$$(-1)^{2k} \equiv 1 \pmod{p}$$

But, $\left(\frac{-1}{p}\right)$ can be ± 1 only. So, $\left(\frac{-1}{p}\right) = 1$

Case 2: $p = 4k + 3, k \in \mathbb{Z}^+$

$$(-1)^{2k+1} \equiv -1 \pmod{p}$$

But, $\left(\frac{-1}{p}\right)$ can be ± 1 only. So, $\left(\frac{-1}{p}\right) = -1$

Combining both cases we prove our statement. □

Theorem 1.5.4 (Gauss's Lemma)**.** *Let p be an odd prime, then:*

i.

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1 \pmod 8 \textit{ or } p \equiv 7 \pmod 8 \\ -1 & \textit{if } p \equiv 3 \pmod 8 \textit{ or } p \equiv 5 \pmod 8 \end{cases}$$

ii.

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1 \pmod{12} \textit{ or } p \equiv 11 \pmod{12} \\ -1 & \textit{if } p \equiv 5 \pmod{12} \textit{ or } p \equiv 7 \pmod{12} \end{cases}$$

Proof. i. Here we can't apply Euler's Criterion in any obvious way, since there doesn't seem to be an easy method to calculate $2^{\frac{p-1}{2}} \pmod p$. Instead we will follow an approach designed by Gauss, which is similar to what we do to prove Fermat's Little Theorem.[7] Here in order to get factor $2^{\frac{p-1}{2}}$ we will multiply each of $1, 2, 3, \dots, \frac{p-1}{2}$ with 2 and then multiply them all together. Then we will take each one of the *double* numbers, $\{2, 4, 6, 8, \dots, (p-1)\}$, that we have generated and calculate their modulo p lying between $-\frac{p-1}{2}$ and $\frac{p-1}{2}$. Then multiply these numbers together and compare with earlier equivalent form to get -1 or $+1$ as answer. Notice that the number of minus signs introduced is exactly the number of times we need to subtract p from residue so as to bring it in our desired range. Hence:[8]

$$2^{\frac{p-1}{2}} \equiv (-1)^{\text{Number of integers in list of double numbers that are larger than } \frac{p-1}{2}} \pmod p$$

Case 1: $p = 8k + 1, k \in \mathbb{Z}^+$

The list of double integers is: $\{2, 4, 6, \dots, 4k, 4k+2, 4k+4, \dots, 8k\}$, hence:
Number of integers in list of double numbers that are larger than $4k$ = Number of even integers[9] between $4k + 2$ and $8k$ (both included) $= 2k$

$$2^{\frac{p-1}{2}} \equiv (-1)^{2k} \equiv 1 \pmod p$$

So, by Euler's Criterion,

$$\left(\frac{2}{p}\right) = 1$$

Case 2: $p = 8k + 3, k \in \mathbb{Z}^+$

The list of double integers is: $\{2, 4, 6, \dots, 4k, 4k+2, 4k+4, \dots, 8k+2\}$, hence:
Number of integers in list of double numbers that are larger than $4k + 1$ = Number of even integers between $4k + 2$ and $8k + 2$ (both included) $= 2k + 1$

$$2^{\frac{p-1}{2}} \equiv (-1)^{2k+1} \equiv -1 \pmod p$$

So, by Euler's Criterion,

$$\left(\frac{2}{p}\right) = -1$$

Case 3: $p = 8k + 5, k \in \mathbb{Z}^+$

The list of double integers is: $\{2, 4, 6, \dots, 4k, 4k+2, 4k+4, \dots, 8k+4\}$, hence:
Number of integers in list of double numbers that are larger than $4k + 2$ = Number of even integers between $4k + 4$ and $8k + 4$ (both included) $= 2k + 1$

$$2^{\frac{p-1}{2}} \equiv (-1)^{2k+1} \equiv -1 \pmod p$$

So, by Euler's Criterion,

$$\left(\frac{2}{p}\right) = -1$$

---

[7] To prove $a^{p-1} \equiv 1 \pmod p$, we multiply each of $1, 2, 3, \dots, p-1$ with a and then multiply them all together, it gives us a factor a^{p-1}.

[8] For illustrations about this method refer pp.171-172 of [16]

[9] This can be calculated by analysis of Arithmetic Progression so formed.

Case 4: $p = 8k + 7, k \in \mathbb{Z}^+$

The list of double integers is: $\{2, 4, 6, \dots, 4k, 4k + 2, 4k + 4, \dots, 8k + 6\}$, hence:

Number of integers in list of double numbers that are larger than $4k + 3$ = Number of even integers between $4k + 4$ and $8k + 6$ (both included) $= 2k + 2$

$$2^{\frac{p-1}{2}} \equiv (-1)^{2k+2} \equiv 1 \pmod p$$

So, by Euler's Criterion,

$$\left(\frac{2}{p}\right) = 1$$

Combining all 4 cases we prove our statement.

ii. Following the same approach as stated in above part we get, list of triple numbers: $\{3, 6, 9, \dots, \frac{3(p-1)}{2}\}$

$$3^{\frac{p-1}{2}} \equiv (-1)^{\text{Number of integers in list of triple numbers that are more than } \frac{p-1}{2} \text{ but less than } p} \pmod p$$

Case 1: $p = 12k + 1, k \in \mathbb{Z}^+$

The list of triple integers is: $\{3, 6, \dots, 9k, 9k + 3, 9k + 6, \dots, 18k\}$, hence:

Number of integers in list of triple numbers that are more than $6k$ but less than $12k+1$ = Number of multiples[10] of 3 between $6k + 3$ and $12k$ (both included) $= 2k$

$$3^{\frac{p-1}{2}} \equiv (-1)^{2k} \equiv 1 \pmod p$$

So, by Euler's Criterion,

$$\left(\frac{3}{p}\right) = 1$$

Case 2: $p = 12k + 5, k \in \mathbb{Z}^+$

The list of triple integers is: $\{3, 6, \dots, 9k, 9k + 3, 9k + 6, \dots, 18k + 6\}$, hence:

Number of integers in list of triple numbers that are more than $6k + 2$ but less than $12k + 5$ = Number of multiples of 3 between $6k + 3$ and $12 + 3k$ (both included) $= 2k + 1$

$$3^{\frac{p-1}{2}} \equiv (-1)^{2k+1} \equiv -1 \pmod p$$

So, by Euler's Criterion,

$$\left(\frac{3}{p}\right) = -1$$

Case 3: $p = 12k + 7, k \in \mathbb{Z}^+$

The list of triple integers is: $\{3, 6, \dots, 9k, 9k + 3, 9k + 6, \dots, 18k + 9\}$, hence:

Number of integers in list of triple numbers that are more than $6k + 3$ but less than $12k + 7$ = Number of multiples of 3 between $6k + 6$ and $12k + 6$ (both included) $= 2k + 1$

$$3^{\frac{p-1}{2}} \equiv (-1)^{2k+1} \equiv -1 \pmod p$$

So, by Euler's Criterion,

$$\left(\frac{3}{p}\right) = -1$$

Case 4: $p = 12k + 11, k \in \mathbb{Z}^+$

The list of triple integers is: $\{3, 6, \dots, 9k, 9k + 3, 9k + 6, \dots, 18k + 15\}$, hence:

Number of integers in list of triple numbers that are more than $6k + 5$ but less than $12k + 11$ = Number of multiples of 3 between $6k + 6$ and $12k + 9$ (both included) $= 2k + 2$

$$3^{\frac{p-1}{2}} \equiv (-1)^{2k+2} \equiv 1 \pmod p$$

So, by Euler's Criterion,

$$\left(\frac{3}{p}\right) = 1$$

---

[10] This can be calculated by analysis of Arithmetic Progression so formed.

Combining all 4 cases we prove our statement.

□

Theorem 1.5.5 (Weak Law of Quadratic Reciprocity)**.** *Let a be any natural number, and express p as $4ak + r$, where $0 < r < 4a$.*

i. Then the quadratic character of $a \pmod p$ is the same for all primes p for which r has the same value.

ii. Moreover the quadratic character of $a \pmod p$ is the same for r and for $4a - r$.

Proof. i. We have to generalize Gauss's Lemma. Consider how many of the numbers:

$$\{a, 2a, 3a, 4a, \ldots, \frac{(p-1)a}{2}\}$$

lie between $\frac{p}{2}$ and p, or between $\frac{3p}{2}$ and $2p$, and so on. Since $\frac{(p-1)a}{2}$ is the largest multiple of a that is less than $\frac{pa}{2}$, the last interval in the series which we have to consider is the interval from $(b - \frac{1}{2})p$ to bp, where b is $\frac{a}{2}$ or $\frac{a-1}{2}$, whichever is an integer.
Thus we have to consider how many multiples of a lie in the intervals:

$$\Big(\frac{p}{2}, p\Big), \Big(\frac{3p}{2}, 2p\Big), \ldots, \Big(\Big(b - \frac{1}{2}\Big)p, bp\Big)$$

None of the numbers occurring here is itself a multiple of a, and so no question arises as to whether any of the endpoints of the intervals is to be counted or not. Dividing throughout by a, we see that the number in question is the total number of integers in all the intervals:

$$\Big(\frac{p}{2a}, \frac{p}{a}\Big), \Big(\frac{3p}{2a}, \frac{2p}{a}\Big), \ldots, \Big(\frac{(2b-1)p}{2a}, \frac{bp}{a}\Big)$$

Now write $p = 4ak + r$.
Since the denominators are all a or $2a$, the effect of replacing p by $4ak + r$ is the same as that of replacing p by r , except that certain even numbers are added to the endpoints of the various intervals. As before, we can ignore these even numbers. It follows that if α is the total number of integers in all the intervals:

$$\Big(\frac{r}{2a}, \frac{r}{a}\Big), \Big(\frac{3r}{2a}, \frac{2r}{a}\Big), \ldots, \Big(\frac{(2b-1)r}{2a}, \frac{br}{a}\Big) \tag{1.5}$$

then a is a quadratic residue or non-residue modulo p according as α is even or odd. The number α depends only on r , and not on the particular prime p which leaves the remainder r when divided by $4a$. This proves first part.

ii. Consider the effect of changing r into $4a - r$. This changes the series of intervals obtained in previous part into the series:

$$\Big(2 - \frac{r}{2a}, 4 - \frac{r}{a}\Big), \Big(6 - \frac{3r}{2a}, 8 - \frac{2r}{a}\Big), \ldots, \Big(4b - 2 - \frac{(2b-1)r}{2a}, 4b - \frac{br}{a}\Big) \tag{1.6}$$

If β denotes the total number of integers in these intervals, we have to prove that α and β are of the same parity.
Observe that intervals $\Big(2 - \frac{r}{2a}, 4 - \frac{r}{a}\Big)$ and $\Big(\frac{r}{2a}, \frac{r}{a}\Big)$ are equivalent as far as parity is concerned.
Now we subtract both numbers of our new interval from 4, we get : $\Big(\frac{r}{a}, 2 + \frac{r}{2a}\Big)$.
Together with the earlier interval $\Big(\frac{r}{2a}, \frac{r}{a}\Big)$, this just makes up an interval of length 2, and such an interval contains exactly 2 integers.
A similar consideration applies to the other intervals in the two series of intervals (1.5) and (1.6), and it follows that $\alpha + \beta$ is even, which proves the result.

□

Theorem 1.5.6 (Law of Quadratic Reciprocity)**.** *If p and q are distinct odd primes of the form $4k + 3$, then one of the congruences $x^2 \equiv p \pmod q$ and $x^2 \equiv q \pmod p$, is solvable and the other is not; but if*

atleast one of the primes is of form $4k+1$, then both congruences are solvable or both are not.
Symbolically: If p and q are distinct odd primes then:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

ALTER: If p and q are distinct odd primes then:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4 \end{cases}$$

Proof. The exponent of -1 on the right is even unless p and q are both of the form $4k+3$.
In previous theorem we proved the quadratic character of a fixed number a to various prime moduli. So we will make use of it here.

Case 1: $p \equiv q \pmod 4$
We can suppose without loss of generality that $p > q$, and we write $p - q = 4a$. Then, since $p = 4a + q$, we have :

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right)$$

Similarly:

$$\left(\frac{q}{p}\right) = \left(\frac{p-4a}{p}\right) = \left(\frac{-4a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)$$

Now $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ are the same, because p and q leave the same remainder on division by $4a$ (and square of both 1 and -1 is 1), hence [see Theorem 1.6.3]:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

ii. $p \not\equiv q \pmod 4$
In this case $p \equiv -q \pmod 4$. Put $p + q = 4a$. Then, we obtain:

$$\left(\frac{p}{q}\right) = \left(\frac{4a-q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right)$$

Similarly:

$$\left(\frac{q}{p}\right) = \left(\frac{4a-p}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{a}{p}\right)$$

Thus $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ are the same, because p and q leave the opposite remainder on division by $4a$ (and square of both 1 and -1 is 1), hence:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$$

Combining both cases, we prove the theorem. □

Now let's consider examples involving diophantine equations:

Example 1.5.1. *Find the solutions of $x^2 - 17y^2 = 12$ in integers.*

Solution. Looking modulo 17 we have

$$x^2 \equiv 12 \pmod{17}$$

By Quadratic Residue Multiplication Rule:

$$\left(\frac{12}{17}\right) = \left(\frac{3}{17}\right)\left(\frac{4}{17}\right) = \left(\frac{3}{17}\right)\left(\frac{2}{17}\right)\left(\frac{2}{17}\right) = \left(\frac{3}{17}\right)$$

Now $3 \equiv 3 \pmod 4$ and $17 \equiv 1 \pmod 4$, thus as per the law of quadratic reciprocity, we have:

$$\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right)$$

This we can calculate easily by reducing 17 modulo 3:

$$\left(\frac{17}{3}\right) = \left(\frac{2}{3}\right)$$

Now we have reduced the solvability of $x^2 \equiv 12 \pmod{17}$ to solvability of $x^2 \equiv 2 \pmod 3$, now clearly this is not solvable[11] since 2 is quadratic non-residue modulo 3, hence:

$$\left(\frac{12}{17}\right) = \left(\frac{2}{3}\right) = -1$$

Hence given diophantine equation is not solvable in integers.

Example 1.5.2. *Let prime p be of form $4k + 3$. Prove that exactly one of equations $x^2 - py^2 = \pm 2$ is solvable.*

Solution. Apply Law of Quadratic Reciprocity to reach conclusion that at most one of given equations is solvable. Then apply modular arithmetic by observing the residue modulo 4 to deduce that atleast one of given equations is solvable.

1.6 Factorization

This method works when we are able to rewrite given diophantine equation as:

$$f_1(x_1, x_2, x_3, \ldots, x_{n_1})f_2(x_1, x_2, x_3, \ldots, x_{n_2}) \ldots f_k(x_1, x_2, x_3, \ldots, x_{n_k}) = a$$

where $a \in \mathbb{Z}$. Then *given* prime factorization of a we can obtain finitely many decompositions (all combinations), which we can solve as system of diophantine equations. It is generally easier to solve system of diophantine equations rather than single equation because they impose further restrictions on each other apart from having integer or rational number solutions.

Example 1.6.1. *Determine all non-negative integer solutions for:*

$$(xy - 7)^2 = x^2 + y^2$$

Solution. Since there are lot's of squares let's start manipulating given equation:

$$\Rightarrow x^2y^2 - 14xy + 49 = x^2 + y^2$$
$$\Rightarrow (xy - 6)^2 + 13 = (x + y)^2$$
$$\Rightarrow (x + y)^2 - (xy - 6)^2 = 13$$
$$\Rightarrow (x + y - xy + 6)(x + y + xy - 6) = 13$$

yielding the system:

$$\begin{cases} x + y - xy + 6 = 1, \\ x + y + xy - 6 = 13. \end{cases} \qquad \begin{cases} x + y - xy + 6 = 13, \\ x + y + xy - 6 = 1. \end{cases}$$

$$\begin{cases} x + y - xy + 6 = -1, \\ x + y + xy - 6 = -13. \end{cases} \qquad \begin{cases} x + y - xy + 6 = -13, \\ x + y + xy - 6 = -1. \end{cases}$$

Then the non-negative solutions will be : $(3, 4), (4, 3), (0, 7), (7, 0)$ [only first two system are useful].

Example 1.6.2. *Find all integral solutions to the equation:*

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

(Titu Andreescu)

Solution. Take everything to one side, multiply and factorize to get:

$$[xy - 1 - (x - y)]^2 = 4$$

Now obtain all possible system of equations. The solutions will be $(1, 0), (-3, -2), (0, -1), (-2, 3)$.

---

[11] Square all integers from 1 to 2 and find their residues. We get $\{1\}$ as quadratic residue and thus $\{2\}$ as quadratic non-residue.

1.7 Unique Factorization Domains

Here, we will observe some elegant ways of solving diophantine equations using algebra. Firstly let's recall some definitions from algebra:

Definition 1.7.1 (Commutative Ring)**.** A non-empty set R is said to an *commutative ring* if in R there are defined two operations, denoted by $+$ and $*$ respectively such that for all a, b in R:

1. $a + b$ is in R
2. $a + b = b + a$
3. $(a + b) + c = a + (b + c)$
4. There is an element 0 in R such that $a + 0 = a$
5. There exists an element $-a$ in R such that $a + (-a) = 0$ for every a in R.
6. $a * b$ is in R
7. $a * b = b * a$
8. $a * (b * c) = (a * b) * c$
9. $a * (b + c) = (a * b) + (a * c)$ and $(b + c) * a = (b * a) + (c * a)$ for all a, b, c in R

ILLUSTRATION: R is set of even integers under the usual operation of addition and multiplication, R is a *commutative ring.*

Definition 1.7.2 (Zero-divisor)**.** If R is a commutative ring, then $a \neq 0, a \in R$ is said to a *zero-divisor* if there exists a $b \neq 0, b \in R$, such that $ab = 0$.
ILLUSTRATION: $\mathbb{Z}_6$ is a commutative ring with *zero-divisors*, 2, 3 since $\hat{2} * \hat{3} = \hat{0}$.[In general, $\mathbb{Z}_n$ for n not prime has *zero-divisors*.]

Definition 1.7.3 (Integral Domain)**.** A commutative ring is an *integral domain* if it has no zero-divisors.
ILLUSTRATION: $\mathbb{Z}$ is an integral domain.

Definition 1.7.4 (Unique Factorization Domain)**.** An integral domain, R, with unit element[12] is a *unique factorization domain* if:

1. Any non-zero element in R is either a unit or can be written as the product of a finite number of irreducible elements[13] in R
2. The decomposition (done in previous part) is unique upto the order and associates of the irreducible elements.

1.7.1 Gaussian Integers

A class of domains occurring in modern number theory is the class of rings $\mathbb{Z}[\sqrt{d}]$; this consists of all complex numbers of the form $a + b\sqrt{d}$, where a, b are integers and d is any fixed integer (positive or negative) which is not a perfect square and $\sqrt{d}$ is a fixed square root of d in $\mathbb{C}$. When $d = -1$, one calls this the ring of Gaussian integers denoted by $\mathbb{Z}[i]$ where i is a fixed square root of -1 in $\mathbb{C}$. Set of Gaussian integers is:

$$\mathbb{Z}[i] = \{a + bi \quad | \quad a, b \in \mathbb{Z}\}$$

Gaussian integers have many properties in common with ordinary integers. If $\alpha, \beta \in \mathbb{Z}[i]$, then:

1. $\alpha + \beta$ is in $\mathbb{Z}[i]$
2. $\alpha - \beta$ is in $\mathbb{Z}[i]$

---

[12] An element in ring R with a multiplicative inverse is called a *unit element.*

[13] An element a which is not unit in R is called *irreducible* (or *prime element*) if, whenever $a = bc$ with $b, c \in R$, then one of b, c must be a unit in R.

3. $\alpha\beta$ is in $\mathbb{Z}[i]$
4. $\dfrac{\alpha}{\beta}$ is NOT always in $\mathbb{Z}[i]$

Note that like ordinary integers, Gaussian integers also form a commutative ring, and due to absence on zero-divisor, form an integral domain. Now we will prove that this is indeed an unique factorization domain. In fact we can prove that $\mathbb{Z}[\sqrt{-d}]$, $d \geq 3$ is not a Unique Factorization Domain. For proof refer [13].

Definition 1.7.5 (Gaussian Prime)**.** A Gaussian integer α is called *Gaussian prime* if the only integers dividing α are units and α times a unit.

Definition 1.7.6 (Norm)**.** The *norm* of a complex number $\alpha = x + yi$ is defined as, $x^2 + y^2$. Symbolically:

$$N(\alpha) = x^2 + y^2$$

Theorem 1.7.1 (Gaussian Unit Theorem)**.** *The only units in the Gaussian integers are* $1, -1, i$ *and* $-i$. *That is, these are the only Gaussian integers that have Gaussian integer multiplicative inverses.*

Proof. Suppose that $a + bi$ is a unit in the Gaussian integer. Thus, it has a multiplicative inverse, so there is another Gaussian integer $c + di$ such that

$$\Rightarrow (a + bi)(c + di) = 1$$

$$\Rightarrow (ac - bd) + (ad + bc)i = 1$$

Now equating real and imaginary parts we get:

$$\begin{cases} ac - bd = 1, \\ ad + bc = 0 \end{cases}$$

We will look for integer a, b which satisfy this set of equations. Consider three cases:

Case 1: $a = 0$

$$\Rightarrow bd = -1 \quad \Rightarrow b = \pm 1$$

Thus, $a + bi = \pm i$

Case 2: $b = 0$

$$\Rightarrow ac = 1 \quad \Rightarrow a = \pm 1$$

Thus, $a + bi = \pm 1$

Case 3: $a, b \neq 0$

$$\Rightarrow c = \frac{1 + bd}{a}$$

Using this in second equation of our set:

$$\Rightarrow \frac{a^2 d + b + b^2 d}{a} = 0$$

Thus any solution with $a \neq 0$ must satisfy:

$$(a^2 + b^2)d = -b$$

Thus, $a^2 + b^2$ divides b, which is absurd, since $a^2 + b^2$ is larger than b (since neither a nor b is 0). This means that Case 3 yields no new units, so we have completed the proof.

□

Theorem 1.7.2 (Norm Multiplication Property)**.** *Let α and β be any complex numbers. Then:*

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

Proof. Let:

$$\begin{cases} \alpha = a + bi \\ \beta = c + di \end{cases}$$

where, $a, b, c, d \in \mathbb{Z}$. Then:

$$\alpha\beta = (ac - bd) + ad + bc)i$$

Further:

$$N(\alpha) = a^2 + b^2 \quad \text{and} \quad N(\beta) = c^2 + d^2$$

Also:

$$N(\alpha\beta) = (ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2)$$

□

Remark: This also proves that a Gaussian integer α is a unit if and only if $N(\alpha) = 1$.

Theorem 1.7.3 (Gaussian Prime Theorem)**.** *The Gaussian primes can be described as follows:*

(i) $1 + i$ *is a Gaussian prime.*

(ii) Let p be an ordinary prime[14] *with $p \equiv 3 \pmod 4$. Then p is a Gaussian prime.*

(iii) Let p be an ordinary prime with $p \equiv 1 \pmod 4$ and write p as a sum of two squares[15]*, $p = u^2 + v^2$. Then $u + vi$ is a Gaussian prime.*

Proof. Firstly, we define a method for factoring a Gaussian integer, α as:
Set, α as product of two Gaussian integers:

$$\alpha = (a + bi)(c + di)$$

Now take norm of both sides:

$$N(\alpha) = (a^2 + b^2)(c^2 + d^2)$$

This is an equation in integers, and we want a non-trivial solution, i.e. neither $a^2 + b^2$ nor $c^2 + d^2$ equals 1. Thus:

$$\begin{cases} a^2 + b^2 = A \\ c^2 + d^2 = B \end{cases}$$

where $A, B \neq 1$, and we need to solve these diophantine equations in order to factorize Gaussian integer.

(i) Put, $\alpha = 1 + i$ to get, $2 = AB$, with ordinary integers $A, B > 1$. But 2 can't be factored in this way. Thus, α has no non-trivial factorizations in the Gaussian integers, so it is prime.

(ii) Let $\alpha = p$ be an ordinary prime with $p \equiv 3 \pmod 4$. Then $p^2 = AB$ and

$$\begin{cases} a^2 + b^2 = A = p \\ c^2 + d^2 = B = p \end{cases}$$

But p can be written as a sum of two squares exactly when $p \equiv 1 \pmod 4$ [proof of this statement comes from quadratic reciprocity and infinite descent method]. Since, $p \equiv 3 \pmod 4$ it can't be written as sum of two square, so there are no solutions. Therefore, p cannot be factored, so it is a Gaussian prime.

(iii) Let $u + iv = \alpha$. Then $N(\alpha) = p = AB$, with ordinary integers $A, B > 1$. But p can't be factored in this way. Thus, α has no non-trivial factorizations in the Gaussian integers, so it is prime.

---

[14] Ordinary primes are the primes integers like $2, 3, 5, 7, 11, \ldots, 101, \ldots$

[15] Let p be a prime, then p is a sum of two squares exactly when $p \equiv 1 \pmod 4$ or $p = 2$. For proof see pp. 188 of [16]

□

Theorem 1.7.4 (Gaussian Integer Division Theorem)**.** *For any $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, there are $\gamma, \delta \in \mathbb{Z}[i]$ such that:*

$$\alpha = \beta\gamma + \delta \quad \textit{and} \quad N(\delta) < N(\beta)$$

Proof. Divide the equation we're trying to prove by β to get:

$$\frac{\alpha}{\beta} = \gamma + \frac{\delta}{\beta} \quad \text{and} \quad N\left(\frac{\delta}{\beta}\right) < 1$$

The norm on $\mathbb{Z}[i]$ is closely related to the absolute value on $\mathbb{C}$, $N(a + bi) = |a + bi|^2$. The absolute value on $\mathbb{C}$ is a way of measuring distances in $\mathbb{C}$.
In $\mathbb{C}$, the farthest a complex number can be from an element of $\mathbb{Z}[i]$ is $1/\sqrt{2}$, since the center points of 1×1 squares with vertices in $\mathbb{Z}[i]$ are at distance $1/\sqrt{2}$ from the vertices.
Now consider the ratio α/β as a complex number and place it in a 1×1 square having vertices in $\mathbb{Z}[i]$.
Let $\gamma \in \mathbb{Z}[i]$ be the vertex of the square that is nearest to α/β, so

$$\left|\frac{\alpha}{\beta} - \gamma\right| \leq \frac{1}{\sqrt{2}}$$

$$\Rightarrow \left|\frac{\delta}{\beta}\right| \leq \frac{1}{\sqrt{2}}$$

Squaring both sides and recalling that the squared complex absolute value on $\mathbb{Z}[i]$ is the norm, we obtain:

$$N\left(\frac{\delta}{\beta}\right) \leq \frac{1}{2} < 1$$

□

Theorem 1.7.5 (Gaussian Integer Common Divisor Property)**.** *Let α and β be Gaussian integers, then consider following sets:*

$$A = \{a : a \in \mathbb{Z}[i]\} \quad \textit{and} \quad B = \{b : b \in \mathbb{Z}[i]\}$$

We define:

$$S = A\alpha + B\beta = \{s = a\alpha + b\beta : a \in A, b \in B\}$$

Then among all the Gaussian integers in S, let, $g = a\alpha + b\beta$ be an element having the smallest non-zero norm. Then g divides both α and β.

Proof. According to Gaussian Integer Division Theorem we can divide α by g:

$$\alpha = g\gamma + \delta \quad \text{with} \quad 0 \leq N(\delta) < N(g)$$

Substituting: $g = a\alpha + b\beta$, we get:

$$\Rightarrow \alpha = a\alpha\gamma + b\beta\gamma + \delta$$

Rearranging terms we get:

$$\Rightarrow \delta = (1 - a\gamma)\alpha + (-b\gamma)\beta$$

Thus, $\delta \in S$. But, $N(\delta) < N(g)$ and $N(g) > 0$ is smallest possible norm in S. Thus, $N(\delta) = 0$ and $\delta \notin S$. Hence,

$$\alpha = g\gamma \quad \Rightarrow g\big|\alpha$$

Similar argument shows, $g\big|\beta$ □

Theorem 1.7.6 (Gaussian Prime Divisibility Theorem)**.** *Let π be a Gaussian prime, if π divides a product $\alpha_1\alpha_2\alpha_3 \ldots \alpha_n$ of Gaussian integers, then it divides atleast one of the factors $\alpha_1\alpha_2\alpha_3 \ldots \alpha_n$.*

Proof. We will prove it by induction.
Consider, $n = 2$. Thus, $\pi \big| AB$. Apply the Gaussian Integer Common Divisor Property to the two numbers A and π. Thus we can find Gaussian integers a and b such that:

$$g = aA + b\pi \tag{1.7}$$

divides both A and π. But π is a prime, thus:

$$g \big| \pi \quad \Rightarrow g = u\pi \quad \text{or} \quad g = u$$

where u in Gaussian unit. Thus we have two cases:

Case 1: $g = u\pi$
Since, $u = \{1, -1, i, -i\}$, and $g \big| A$, so π clearly divides A and given theorem is proved for this case.

Case 2: $g = u$
Multiply the equation (1.7) by another Gaussian integer B to get:

$$gB = aAB + b\pi B$$

But, we are given that, $\pi \big| AB$, and g is unit, so

$$\pi \big| gB \quad \Rightarrow \pi \big| B$$

This proves given theorem for Case 2.

Combining Case 1 and Case 2, we prove given theorem for $n = 2$.
Now suppose that we have proved the Gaussian Prime Divisibility Theorem for all products having fewer than n factors, and suppose that π divides a product $\alpha_1\alpha_2\alpha_3 \ldots \alpha_n$ having n factors.
Let $A = \alpha_1 \ldots \alpha_{n-1}$ and $B = \alpha_n$, then π divides AB, so we know from above that either π divides A or π divides B.
If π divides B, then we're done, since $B = a_n$.
On the other hand, if π divides A, then π divides the product $\alpha_1\alpha_2\alpha_3 \ldots \alpha_{n-1}$ consisting of $n - 1$ factors, so by the induction hypothesis we know that π divides one of the factors $\alpha_1\alpha_2\alpha_3 \ldots \alpha_{n-1}$.
This completes the proof of the theorem. □

Theorem 1.7.7 (Unique Factorization of Gaussian Integers)**.** *Every Gaussian integer $\alpha \neq 0$ can be factored into a unit u multiplied by a product of normalized Gaussian primes in exactly one way.*

$$\alpha = u\pi_1^{e_1}\pi_2^{e_2}\pi_3^{e_3} \ldots \pi_n^{e_n} = u\prod_{r=1}^{n} \pi_r^{e_r}$$

where $\pi_1, \pi_2, \ldots, \pi_n$ are distinct Gaussian primes and $e_1, e_2, \ldots, e_n > 0$ are exponents. Thus if α is itself a unit then, factorization of α will be simply, $\alpha = u$.

Proof. The proof is in two parts:

Part 1: *Every Gaussian integers has some factorization into primes*

Let, there exist at least one non-zero Gaussian integer that doesn't factor into primes.
Among the non-zero Gaussian integers with this property, choose the Gaussian integer having smallest norm, call it α. We can do this, since the norms of non-zero Gaussian integers are positive integers, and any collection of positive integers has a smallest element.
Note that α cannot itself be prime, since otherwise $\alpha = \alpha$ is already a factorization of a into primes.
Similarly, α cannot be a unit, since otherwise $\alpha = \alpha$ would again be a factorization into primes (in this case, into zero primes).
But if α is neither prime nor a unit, then it must factor into a product of two Gaussian integers β, γ, neither of which is a unit:

$$\alpha = \beta\gamma$$

Now consider the norms of β and γ Since β and γ are not units, we know that $N(\beta) > 1$ and $N(\gamma) > 1$. We also have the multiplication property $N(\beta)N(\gamma) = N(\alpha)$, so

$$N(\beta) = \frac{N(\alpha)}{N(\gamma)} < N(\alpha) \quad \text{and} \quad N(\gamma) = \frac{N(\alpha)}{N(\beta)} < N(\alpha)$$

But we chose α to be the Gaussian integer of smallest norm that does not factor into primes, so both β and γ do factor into primes:

$$\beta = u\prod_{r=m}^{n} \pi_r^{e_r} \quad \text{and} \quad \gamma = u'\prod_{r=i}^{j} \pi_r^{e_r}$$

for certain Gaussian primes, $\pi_m, \pi_{m+1}, \ldots, \pi_n, \pi_i, \pi_{i+1}, \ldots, \pi_j$. But then:

$$\alpha = u\pi_1^{e_1}\pi_2^{e_2}\pi_3^{e_3}\ldots\pi_p^{e_p} = u\prod_{r=1}^{p} \pi_r^{e_r}$$

is also a product of primes, which contradicts the choice of α as a number that cannot be written as a product of primes.
Thus, every non-zero Gaussian integer does factor into primes.

Part 2: *The factorization into primes can be done in only one way.*

Let, there exists at least one non-zero Gaussian integer with two distinct factorizations into primes. Among the non-zero Gaussian integers with this property, choose the Gaussian integer having smallest norm, call it α. We can do this, since the norms of non-zero Gaussian integers are positive integers, and any collection of positive integers has a smallest element.
Thus, α has two factorizations:

$$\alpha = u\prod_{r=m}^{n} \pi_r^{e_r} = u'\prod_{r=i}^{j} \pi_r^{e_r}$$

Clearly, α can't be unit, since otherwise, $\alpha = u = u'$, so the factorization wouldn't be different.
This means that: $n - m + 1 \geq 1$, so there is a prime π_m in the first factorization. Then:

$$\pi_m \big| \alpha \quad \Rightarrow \pi_m \left| u'\prod_{r=i}^{j} \pi_r^{e_r} \right.$$

The Gaussian Prime Divisibility Theorem tells us that π_m divides at least one of the numbers, $u', \pi_i, \pi_{i+1}, \ldots, \pi_j$. It certainly doesn't divide the unit, u', so it divides one of the factors. Rearranging the order of these other factors, we may assume that π_m divides π_i. However, the number π_i is a Gaussian integer prime, so its only divisors are units and itself times units. Since π_m is not a unit:

$$\pi_m = (\text{unit}) \times \pi_i$$

Further, both π_m and π_i are normalized,so the unit must equal 1 and $\pi_m = \pi_i$.
Let,

$$\beta = \frac{\alpha}{\pi_m} = \frac{\alpha}{\pi_i}$$

Cancelling π_m and π_i from two factorizations of α yield:

$$\beta = u\prod_{r=m+1}^{n} \pi_r^{e_r} = u'\prod_{r=i+1}^{j} \pi_r^{e_r}$$

Thus, β has two distinct factorizations into prime. But,

$$N(\beta) = \frac{N(\alpha)}{N(\pi_m)} < N(\alpha)$$

This contradicts our assumption that α is the Gaussian integer with smallest norm having two different factorizations into primes, hence our original statement must be false. So every Gaussian integer has a unique such factorization.

□

Example 1.7.1. *Solve the equation in positive integers:*

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

where x, y, z are pairwise prime (non-trivial primitive solutions).

Solution. Suppose that (x_1, y_1, z_1) is a non-trivial primitive solution to given equation with $\gcd(x_1, y_1) = 1$. Thus one of x_1 and y_1 is odd and hence z_1 is odd. We can rewrite given equation in $\mathbb{Z}[i]$ as:

$$(x_1 + iy_1)(x_1 - iy_1) = z_1^2$$

Now, let, $\gcd(x_1 + iy_1, x_1 - iy_1) = d$, where, $d \in \mathbb{Z}[i]$ be irreducible. Then,

$$d\Big|\Big((x_1 + iy_1) - (x_1 - iy_1)\Big) \quad \Rightarrow d\Big|2iy_1$$

Similarly,

$$d\Big|\Big((x_1 + iy_1) + (x_1 - iy_1)\Big) \quad \Rightarrow d\Big|2x_1$$

But, since, z_1 is odd, $d \not\Big|2$, so,

$$d\Big|iy_1 \quad \text{and} \quad d\Big|x_1$$

Taking norms we can say:

$$N(d)\Big|y_1^2 \quad \text{and} \quad N(d)\Big|x_1^2$$

But, $\gcd(x_1, y_1) = 1$, and a Gaussian integer is a unit if and only if its norm is one [see "Norm Multiplication Property"]. Thus $d = u$ where u is unit Gaussian integer. Hence $x_1 + iy_1$ and $x_1 - iy_1$ are relatively prime in $\mathbb{Z}[i]$.
Hence both $x_1 + iy_1$ and $x_1 - iy_1$ are perfect squares, consider any one:

$$x_1 + iy_1 = u(a + ib)^2 = u\Big(\big(a^2 - b^2\big) + i\big(2ab\big)\Big)$$

for some unit $u \in \{-1, 1, i, -i\}$ and some positive integers a, b.
Since we are solving for positive integers, let $u = 1$, [by taking other values of u you will get similar expressions for x_1, y_1, z_1] thus:

$$\begin{cases} x_1 = a^2 - b^2 \\ y_1 = 2ab \end{cases}$$

therefore, $z_1 = a^2 + b^2$, but since z_1 is odd, so a and b are of different parity.

Example 1.7.2. *Solve the equation in integers:*

$$x^2 + 4 = y^3$$

Solution. We will consider two cases based on parity of x.

Case 1: *x is odd.*

The equation can be written in $\mathbb{Z}[i]$ as:

$$(2 + ix)(2 - ix) = y^3 \tag{1.8}$$

Let $z = \gcd(2 + ix, 2 - ix)$, $z = c + di \in \mathbb{Z}[i]$. Then:

$$z\Big|\Big((2 + ix) + (2 - ix)\Big) \quad \Rightarrow z\Big|4 \quad \Rightarrow (c + id)\Big|4$$

Further, then:

$$(c - id)\Big|4 \quad \Rightarrow \bar{z}\Big|4$$

Thus:

$$z \cdot \bar{z}\Big|16 \quad \Rightarrow (c^2+d^2)\Big|16 \tag{1.9}$$

On the other hand[16]

$$z\Big|(2+ix) \quad \Rightarrow \bar{z}\Big|(2-ix)$$

Thus:

$$z \cdot \bar{z}\Big|4+x^2 \quad \Rightarrow (c^2+d^2)\Big|(4+x^2) \tag{1.10}$$

Now since x is odd, so comparing (1.10) and (1.9) we get,

$$c^2+d^2=1$$

Hence, $z=u$, where u is a unit Gaussian integer. Thus, $(2+ix)$ and $(2-ix)$ are relatively prime in $\mathbb{Z}[i]$.
Because $(2+ix)$ and $(2-ix)$ are relatively prime, from (1.8) it follows that

$$2+ix=(a+bi)^3$$

for some integers a and b.[let unit Gaussian integer to be 1, as did in previous example]
Identifying the real and imaginary parts, we get

$$\begin{cases} a(a^2-3b^2)=2 \\ 3a^2b-b^3=x \end{cases}$$

The first equation leads to our general *factorization* method illustrated in Section 1.6, thus giving system of equations

$$\begin{cases} a=1 \\ a^2-3b^2=2 \end{cases} \qquad \begin{cases} a=-1 \\ a^2-3b^2=-2 \end{cases}$$

$$\begin{cases} a=2 \\ a^2-3b^2=1 \end{cases} \qquad \begin{cases} a=-2 \\ a^2-3b^2=-1 \end{cases}$$

gives $a=-1, b=\pm 1$ or $a=2, b=\pm 1$, yielding $x=\pm 2, \pm 11$ but x is odd, thus we consider, $x=\pm 11$ only, and $y=5$.

Case 2: *x is even.*

Then y is even.
Let $x=2u$ and $y=2v$. The equation becomes:

$$u^2+1=2v^3 \quad \Rightarrow (u+i)(u-i)=2v^3$$

By similar argument as used above, $\gcd(u+i,u-i)=1$ and $2=(1+i)(1-i)$. Now using again the uniqueness of prime factorization in $\mathbb{Z}[i]$, we obtain:

$$u+i=(1+i)(a+bi)^3$$

for some integers a and b.
Identifying the real and imaginary parts, we get:

$$\begin{cases} a^3-3a^2b-3ab^2+b^3=u, \\ a^3+3a^2b-3ab^2-b^3=1. \end{cases}$$

The second relation can be written as:

$$(a-b)(a^2+4ab+b^2)=1,$$

---

[16] Recall that if x, y are complex numbers then :

$$\frac{x}{y}=\frac{x\bar{y}}{|y|^2}$$

leading to our general *factorization* method illustrated in Section 1.6, thus yielding system of equations:

$$\begin{cases} a-b=1 \\ a^2+4ab+b^2=1 \end{cases} \qquad \begin{cases} a-b=-1 \\ a^2+4ab+b^2=1 \end{cases}$$

gives $a=1, b=0$ and $a0, b=-1$ [second system have no solution by modular arithmetic argument, modulo 3], yielding $x=2, y=2$ and $x=-22, y=2$
Thus all solutions are $(-11,5), (-2,2), (2,2), (11,5)$.

1.7.2 Ring of integers of $\mathbb{Q}[\sqrt{d}]$

In previous section we saw a special case of the rings $\mathbb{Z}[\sqrt{d}]$ for square-free d. Note that any element of this kind of ring is $u = a + b\sqrt{d}$ which is a root of the polynomial $(X-a)^2 - db^2$; this is a polynomial which has integer coefficients and is monic (i.e., has top coefficient 1). Such complex numbers go under the name of *algebraic integers*. Thus, elements of $\mathbb{Z}[\sqrt{d}]$ are algebraic integers.
But we need to study the set of all the algebraic integers in a particular number field like $\mathbb{Q}[\sqrt{d}]$.

$$\mathbb{Q}[\sqrt{d}] = \{m + n\sqrt{d} : m, n \in \mathbb{Q}\}$$

where d is a non-zero square free integer.
In $\mathbb{Q}[\sqrt{d}]$, the ring of all algebraic integers may be larger than $\mathbb{Z}[\sqrt{d}]$.For instance, for $d=-3$, the number $\frac{1}{2} + \frac{\sqrt{-3}}{2}$ is also an algebraic integer (note that $-3 \equiv 1 \pmod 4$) . One calls the set of all algebraic integers in $K = \mathbb{Q}[\sqrt{d}]$ the ring of integers of K.
Let's define certain terms before we proceed:

Definition 1.7.7 (Conjugate)**.** If $\mu \in \mathbb{Q}[\sqrt{d}]$, such that, $\mu = a + b\sqrt{d}$, then another element of $\mathbb{Q}[\sqrt{d}]$, $a - b\sqrt{d}$, is called *conjugate* of μ, denoted by $\bar{\mu}$.

Definition 1.7.8 (Norm Function)**.** A function, $N : \mathbb{Q}[\sqrt{d}] \to \mathbb{Z}$ is called norm Function in $\mathbb{Q}[\sqrt{d}]$, if for all $\mu \in \mathbb{Q}[\sqrt{d}]$, $N(\mu) = \mu \cdot \bar{\mu}$. Thus,

$$\mu = a + b\sqrt{d} \quad \overset{N(\mu)}{\longmapsto} \quad a^2 - db^2$$

Theorem 1.7.8. *If $d \equiv 2, 3 \pmod 4$, then the ring of integers of $\mathbb{Q}[\sqrt{d}]$ is*

$$\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d}$$

If $d \equiv 1 \pmod 4$, then the ring of integers of $\mathbb{Q}[\sqrt{d}]$ is

$$\mathbb{Z}\left[\frac{(-1+\sqrt{d})}{2}\right] = \mathbb{Z} + \mathbb{Z}\frac{(-1+\sqrt{d})}{2}$$

Proof. Consider an algebraic integer:

$$\mu = \frac{a + b\sqrt{d}}{c}$$

where, $a, b, c \in \mathbb{Z}$, $c > 0$ and $\gcd(a, b, c) = 1$.
If $b = 0$, then: $\mu = a/c$ is rational, then $c = 1$ and we get a rational integer.[17]
If, $b \neq 0$, then μ is root of following quadratic equation:

$$(cx - a)^2 = db^2 \quad \Rightarrow c^2x^2 - 2acx + a^2 - db^2 = 0$$

Divide this equation by c^2 to get monic polynomial:

$$\Rightarrow x^2 - \frac{2a}{c}x + \frac{a^2 - db^2}{c^2} = 0$$

In, the field $\mathbb{Q}[\sqrt{d}]$, we get:

$$c^2 \big| (a^2 - db^2) \quad \text{and} \quad c \big| 2a$$

---

[17] Rational integer is another name for $\mathbb{Z}$.

Consider the first result and let $\gcd(a,c)=r$, then we get:

$$r^2 \big| a^2 \quad \text{and} \quad r^2 \big| c^2 \quad \Rightarrow r^2 \big| (a^2 - db^2) \quad \Rightarrow r^2 \big| db^2 \quad \Rightarrow r \big| b$$

Since, d is a non-square integer. But, $\gcd(a,b,c)=1$, thus $r=1$.
Now, consider the second result. Since $c\big|2a$, we have $c=1$ or $c=2$.
If, $c=2$, then a is odd since $\gcd(a,c)=1$ and

$$db^2 \equiv a^2 \equiv 1 \pmod 4$$

so, b is odd and $d \equiv 1 \pmod 4$.
Now we can consider two cases:

Case 1: $d \not\equiv 1 \pmod 4$ or $d \equiv 2, 3 \pmod 4$ [since d is square free]

Then, $c=1$ and the integers of $\mathbb{Q}[\sqrt{d}]$ are:

$$\mu = a + b\sqrt{d}$$

with rational integral a, b.

Case 2: $d \equiv 1 \pmod 4$

An algebraic integer of $\mathbb{Q}[\sqrt{d}]$ is:

$$\eta = \frac{-1+\sqrt{d}}{2}$$

and all algebraic integers can be expressed simply in terms of this η.
If $c=2$, then a, b are odd and

$$\mu = \frac{a+b\sqrt{d}}{2} = \frac{a+b}{2} + b\eta = a_1 + (2b_1+1)\eta$$

where a_1, b_1 are rational integers.
If $c=1$, then

$$\mu = a + b\sqrt{d} = (a+b) + 2b\eta = a_1 + 2b_1\eta$$

where a_1, b_1 are rational integers.
Thus, if we change our notation a little, the integers of $\mathbb{Q}[\sqrt{d}]$ are the numbers $a + b\eta$, with rational integral a, b.

Combining both cases we prove our theorem. $\square$

Theorem 1.7.9. *The ring of integers in $\mathbb{Q}[\sqrt{d}]$ with $d<0$ and square-free is a Unique Factorization Domain (UFD) exactly when $d \in \{-1,-2,-3,-7,-11,-19,-43,-67,-163\}$*

Remark about Proof. It was proved by Gauss that the ring of integers of quadratic field $\mathbb{Q}[\sqrt{-d}]$ is a UFD for $d = \{1,2,3,7,11,19,43,67,163\}$. Gauss also conjectured that for no other positive square-free d is the ring of integers of $\mathbb{Q}[\sqrt{-d}]$ a UFD. This conjecture was proved, after about 150 years, in 1966 by A. Baker and H. M. Stark independently.
For proof of this theorem refer [3]. Since it uses advance concepts from analysis, it is out of scope of this project to discuss its proof.

Theorem 1.7.10. *Let $d<0$ be a square-free integer, and U_d denote the set of units in corresponding ring of integers of $\mathbb{Q}[\sqrt{d}]$ then:*

1. $U_s = \{1,-1\}$, *for* $s = \{-2,-7,-11,-19,-43,-67,-163\}$.
2. $U_1 = \{1,-1,i,-i\}$
3. $U_3 = \{1,-1,\omega,-\omega,\omega^2,-\omega^2\}$ *where* $\omega = \frac{-1+\sqrt{-3}}{2}$ *is cube root of unity.*

Sketch of Proof. .

1. Prove and use the multiplicative property of norm function. And get ±1 as units of all values of d
2. Since, $-1 \equiv 3 \pmod 4$, we get ring of integers of $\mathbb{Q}[\sqrt{-1}]$ as $\mathbb{Z}[i]$, thus proof is same as that of Gaussian Unit Theorem.
3. $-3 \equiv 1 \pmod 4$ so, use Theorem 1.7.8 and generate appropriate diophantine equations. You will find for $d \equiv 1 \pmod 4$ that equation will be solvable only for $d = -3$. Solve that equation and get the other units (apart from ±1) of $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$.

Example 1.7.3. *Solve the equation in integers*[18]

$$x^3 - 2 = y^2$$

Solution. Re-write given equation as:

$$x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2})$$

Note that both x and y must be odd (since x, y should be of same parity and if y is even $y^2 + 2 \equiv 2 \pmod 4$, and no cube is $\equiv 2 \pmod 4$).
Now let $r = \gcd\big((y + \sqrt{-2}), (y - \sqrt{-2})\big)$.

$$\Rightarrow r\big|\big((y + \sqrt{-2}) - (y - \sqrt{-2})\big) \quad \Rightarrow r\big|2\sqrt{-2}$$

Thus r is a power of $\sqrt{-2}$.
On the other hand, if $\sqrt{-2}\big|(y \pm \sqrt{-2})$, then

$$r\big|(y + \sqrt{-2})(y - \sqrt{-2}) \quad \Rightarrow r\big|(y^2 + 2) \quad \Rightarrow r\big|x^3$$

But x is odd; hence $\sqrt{-2} \not| r$.
We have seen that $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ are relatively prime and that their product is a cube. Since the ring of integers of $\mathbb{Q}[\sqrt{-2}]$ i.e. $\mathbb{Z}[\sqrt{-2}]$ is a UFD (since $-2 \equiv 2 \pmod 4$), this implies that the factors are cubes up to units.
Since the only units are ±1 and these are cubes, it follows that

$$y + \sqrt{-2} = \big(a + b\sqrt{-2}\big)^3$$

Comparing real and imaginary parts, we obtain:

$$\begin{cases} y = a^3 - 6ab^2 \\ 1 = 3a^2b - 2b^3 \end{cases}$$

Now we will apply *Factorization* method of Section 1.6 to second equation and get the system of equations:

$$\begin{cases} b = 1 \\ 3a^2 - 2b^2 = 1 \end{cases} \qquad \begin{cases} b = -1 \\ 3a^2 - 2b^2 = -1 \end{cases}$$

Thus yielding $a = \pm 1, b = 1$ as solution.
Substitute this in first equation to get: $y = \pm 5$
Further, use this in given equation to get: $x = 3$.
Thus, $(3, -5)$ and $(3, 5)$ are only integer solutions of this equation.

Example 1.7.4. *Solve the equation in integers:*

$$x^2 + x + 2 = y^3$$

Solution. Factorize the quadratic part, observe that the greatest common factor of these factors is 1 (lengthy argument). Now use uniqueness of the prime factorization in the ring of integers of $\mathbb{Q}[\sqrt{-7}]$. Follow the approach used in previous example and get $(2, 2)$ and $(-3, 2)$ as only solutions of the given equation.

---

[18] An interesting account on this problem can be found on pp. 77 of [2]

1.8 Rational Points on Elliptic Curves

Once a single solution has been identified for given equation, by using concept of Rational Points on Curves all other solutions can be identified.[19]. In this section we will concentrate only on *non-singular cubic curves.* Let's start we some definitions:

Definition 1.8.1 (Rational Point)**.** A point with both of it's coordinates as rational numbers is called a *rational point.*

Definition 1.8.2 (Homogeneous Coordinates)**.** Two triples $[a, b, c]$ and $[a', b', c']$ are considered to be same point, if there is a non-zero t such that $a = ta', b = tb', c = tc'$. Then the number a, b, c are caled *homogeneous coordinates* for point $[a, b, c]$.

Definition 1.8.3 (Projective Plane (Algebraic Definition))**.** We denote projective plane by $\mathbb{P}^2$ and define an equivalence relation $\sim$ such that, $[a, b, c] \sim [a', b', c']$ if there is non-zero t so that $a = ta', b = tb', c = tc'$. Thus $\mathbb{P}^2$ consists of the set of all equivalence classes of triples $[a, b, c]$ except $[0, 0, 0]$. Symbolically:

$$\mathbb{P}^2 = \frac{\{[a, b, c] : a, b, c \quad \text{are not all zero}\}}{\sim}$$

Definition 1.8.4 (Line in Projective Plane)**.** The set of points $[a, b, c] \in \mathbb{P}^2$ whose coordinates satisfy an equation of form:

$$\alpha X + \beta Y + \gamma Z = 0$$

where α, β, γ are all non-zero constants and $[X, Y, Z]$ are any homogeneous coordinates for the point.

Definition 1.8.5 (Affine Plane)**.** An ordinary plane of elementary plane geometry, in which two lines are said to be parallel if they do not meet. It is denoted by $\mathbb{A}^2$.

Definition 1.8.6 (Set of Directions in $\mathbb{A}^2$)**.** Every set of line in $\mathbb{A}^2$ is parallel to a unique line through the origin, thus the set of lines in $\mathbb{A}^2$ going through origin are defined as *set of directions in* $\mathbb{A}^2$. This set denoted by $\mathbb{P}^1$, since set of directions in $\mathbb{A}^2$ is $[a, b]$ of the projective line $\mathbb{P}^1$.

Definition 1.8.7 (Projective Plane (Geometric Definition))**.** Projective plane, $\mathbb{P}^2$, is union of affine plane, $\mathbb{A}^2$, and the set of directions in affine plane, $\mathbb{P}^1$. This can be represented as:

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1 = \begin{cases} \left(\frac{a}{c}, \frac{b}{c}\right) \in \mathbb{A}^2 & \text{if } c \neq 0 \\ [a, b] \in \mathbb{P}^1 & \text{if } c = 0 \end{cases}$$

where $[a, b, c]$ is a triple on $\mathbb{P}^2$.
Remark: Thus in $\mathbb{P}^2$ there are no parallel lines.

Definition 1.8.8 (Points at infinity)**.** The extra points in $\mathbb{P}^2$ associated to directions, i.e. the points in $\mathbb{P}^1$ are called *points at infinity.*

Definition 1.8.9 (Algebraic Curve in $\mathbb{A}^2$)**.** The set of real solutions of an equation $f(x, y) = 0$ forms a curve in $\mathbb{A}^2$, called *algebraic curve in* $\mathbb{A}^2$.

Definition 1.8.10 (Projective Curve)**.** Set of solutions of polynomial equation $C : F(X, Y, Z) = 0$ where F is a non-constant homogeneous polynomial[20] forms a curve in $\mathbb{P}^2$, called algebraic curve in $\mathbb{P}^2$ or *projective curve.*

Definition 1.8.11 (Affine part of projective curve)**.** Define a non-homogeneous polynomial $f(x, y)$ from given homogeneous polynomial $F(X, Y, Z)$ such that:

$$C_0 : f(x, y) = F(x, y, 1)$$

Then the curve $f(x, y) = 0$ in $\mathbb{A}^2$ is called *affine part of projective curve.*

---

[19] I will briefly discuss in Section 2.3.4, what happens when the curves are *conic sections.*

[20] A polynomial $F(X, Y, Z)$ is called a homogeneous polynomial of degree d, if it satisfies the identity: $F(tX, tY, tZ) = t^d F(X, Y, Z)$, where $t \neq 0$.

Definition 1.8.12 (Dehomogenization)**.** The process of replacing the homogeneous polynomial $F(X,Y,Z)$ by the inhomogeneous polynomial $f(x,y) = F(x,y,1)$ is called *dehomogenization*, with respect to variable Z.

Definition 1.8.13 (Homogenization)**.** The process of replacing the inhomogeneous polynomial $f(x,y)$ of degree d by the homogeneous polynomial $F(X,Y,Z)$ of degree d is called *homogenization.* Symbolically:

$$f(x,y) = \sum_{i,j} a_{ij} x^i y^j \quad \overset{Homogenization}{\Longrightarrow} \quad F(X,Y,Z) = \sum_{i,j} a_{ij} X^i Y^j Z^{d-i-j}$$

where d is degree of $f(x,y)$.

Definition 1.8.14 (Singular & Non-Singular Point)**.** A point P is singular point of curve $C : f(x,y) = 0$, if:

$$\left.\frac{\partial f}{\partial x}\right|_P = \left.\frac{\partial f}{\partial y}\right|_P = 0$$

else it is called non-singular point.
Remark: For projective curve we check singularity of its affine part.

Definition 1.8.15 (Non-Singular Curve)**.** If every point on a curve is non-singular point then the curve is called non-singular curve.
Remark: Non-singular curves are smooth curves, thus we can define a tangent at every point. Also singular curves are just like conics, we can project them from the point of singularity.

Definition 1.8.16 (Weierstrass Normal Form)**.** Any cubic curve with a rational point can be transformed into a certain special form by a set of projective transformations (i.e. placing the curve in projective plane and choosing it's axis in projective plane) called *Weierstrass Normal Form*, represented as:

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

where a, b, c are rational numbers.

Definition 1.8.17 (Elliptic Curve)**.** Any curve birationally equivalent to a non-singular cubic curve in Weierstrass normal form is called an *elliptic curve.*
Remark: Since curve is non-singular, there is no point on the curve at which partial derivatives vanish simultaneously, thus $f(x)$ can't have double roots. In other words, there can be either one real root of $f(x)$ or three distinct real roots of $f(x)$.

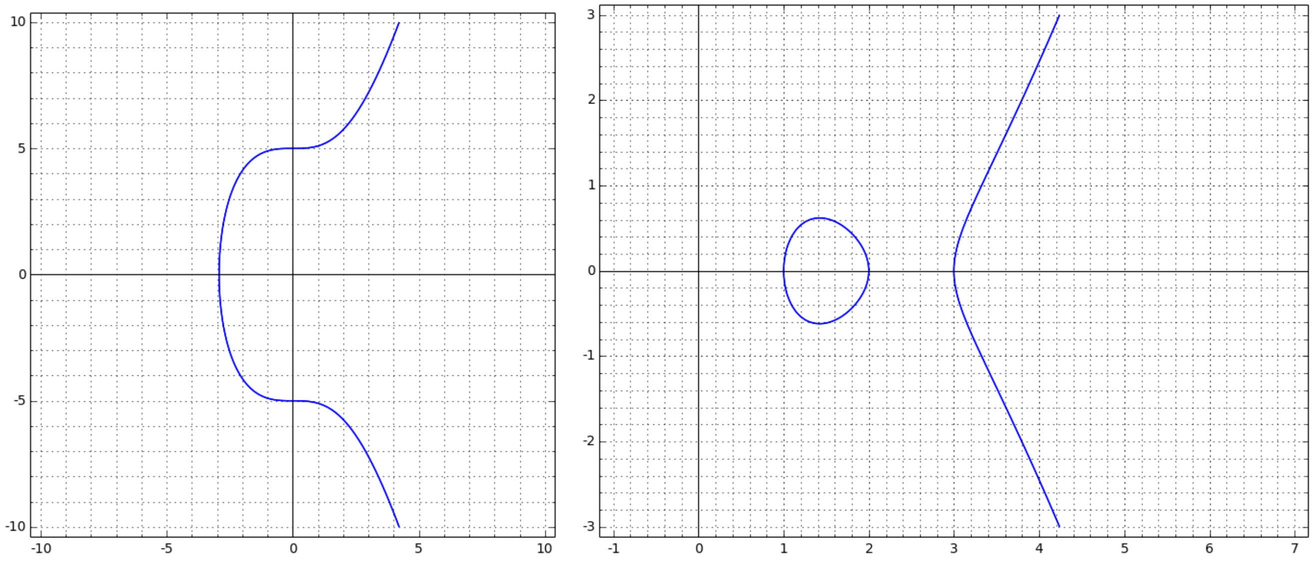

Figure 1.1: These are the possible shapes of elliptic curves. Equation of the curve on left and right hand side is: $y^2 = x^3 + 25$ and $y^2 = x^3 - 6x^2 + 11x - 6$ respectively. [Curves plotted using SageMath Version 6.6]

Commentary on group structure of rational points on a general cubic curve with addition as binary operation[21]

- *What is identity in this group?*
  Any point $\mathcal{O}$ on curve which we use to define : $P+Q = \mathcal{O}*(P*Q)$ is our identity element. (Nothing special about choice of $\mathcal{O}$)

- *What is the inverse ?*
  By drawing tangent at $\mathcal{O}$ and if L is point of intersection of that tangent with curve then $\mathcal{O}*L = \mathcal{O}$ since we had allowed multiplicities of intersections (counting points of tangency as intersections of multiplicity greater than one). Using this fact we can find inverses.

- *Is the group commutative?*
  The operation $*$ could not form a group just because it didn't have an identity element (since identity element for $*$ exists only in special cases when one of points in consideration is tangent point). But $*$ operation is commutative (since it doesn't matter from which point we start drawing a line), so the composition of commutative operation will also yield a commutative operation i.e. $+$ is a commutative operation.

- *How to prove associative property?*
  Showing $P+(Q+R) = (P+Q)+R$ is equivalent to showing $\mathcal{O}*(P*(\mathcal{O}*(Q*R))) = \mathcal{O}*((\mathcal{O}*(P*Q))*R)$ i.e. $P*(Q+R) = (P+Q)*R$. Geometrically this leads to two set of lines consisting of 3 lines each and total of nine points (counting final point of intersection). Each set of three lines defines a cubic. So we have two cubics C_1 and C_2 intersecting at nine points and we know that our conic surely passes through 8 of these points (leaving final point of intersection). Now to see that finally both points (RHS and LHS) pass through same point we need to use the theorem : "Let C, C_1, C_2 be three cubic curves. Then if C goes through 8 of 9 intersection points of C_1 and C_2 , then C goes through ninth intersection point also". Hence our conic passes through the final point of intersection. Hence LHS = RHS.

Theorem 1.8.1 (Group Law for points on elliptic curve)**.** *Consider an elliptic curve:*

$$y^2 = x^3 + ax^2 + bx + c$$

Then:

(i) There is only one point at infinity. (call it $\mathcal{O}$)

(ii) If the points on our cubic consists of the ordinary points in the ordinary affine xy plane together with $\mathcal{O}$, counting $\mathcal{O}$ as a rational point and taking it as zero element we make the set of rational points into a (abelian) group with $+$ as binary operation which is composition of $*$ operation. [as defined for addition law of points on general cubic equation]

(iii) If P_1, P_2, are distinct rational points on our curve with $P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_1 * P_2 = (x_3, y_3), P_1 + P_2 = (x_3, -y_3)$, then:

$$\begin{cases} x_3 = \lambda^2 - a - x_1 - x_2 \\ -y_3 = -(\lambda x_3 + \nu) \end{cases}$$

where, $\lambda = \dfrac{y_2 - y_2}{x_2 - x_1}$ *and* $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$

(iv) If $P_0 = (x_0, y_0)$ is a rational point on curve then, $P_0 + P_0 = 2P_0 = (x', y')$, duplication formula, is given by:

$$\begin{cases} x' = \dfrac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c} \\ y' = -(\lambda x' + \nu) \end{cases}$$

where, $\lambda = \frac{3x_0^2 + 2ax_0 + b}{2y_0}$ *and* $\nu = y_0 - \lambda x_0$

---

[21] Refer pp. 15-22 of [10] for proof of group structure of addition law for general cubic curve .

Proof. The proof needs elementary concepts of projective geometry and high-school algebra.

(i) We can homogenize the given equation by getting: $x = \frac{X}{Y}$ and $y = \frac{Y}{Z}$, yielding:

$$Y^2Z = X^3 + ax^2Z + bXZ^2 + cZ^2$$

Now to find the intersection of this point cubic with line at infinity, $Z = 0$, substitute $Z = 0$ into the equation to get:

$$X^3 = 0$$

which has triple root $X = 0$.
This means that the cubic meets the line at infinity in three points, and all these three points are same. So the cubic has exactly one point at infinity, namely, the point at infinity where vertical line ($x = k$, where k is a constant) meet.
The point at infinity is an inflection point of the cubic, and the tangent at that point is the line at infinity, which meets it with multiplicity three.
Also this point is non-singular by the partial derivative test. So for a cubic in given form (Weierstrass form) there is one point at infinity.

(ii) As per given condition every line meets cubic at point $\mathcal{O}$ three times. A vertical line meets the cubic at two points in the xy plane and also at the point $\mathcal{O}$. And a non vertical line meets the cubic in three points in xy plane [allowing x, y to be complex numbers].
Now we can make the general addition law of points on a cubic curve to work on elliptic curves. We are given an equation in Weierstrass form.
Consider two points P, Q on this cubic equation. First we draw the line through P and Q and find the third intersection point $P * Q$. Then we draw the line through $P * Q$ and $\mathcal{O}$, which is just the vertical line through $P * Q$. Since a cubic curve in Weierstrass form is symmetric about x axis, so to find $P + Q$ just take $P * Q$ and reflect it about x axis.

(iii) The equation of line joining (x_1, y_1) and (x_2, y_2) is:

$$y = \lambda x + \nu$$

where $\lambda = \dfrac{y_2 - y_2}{x_2 - x_1}$ and $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$.
By construction, the line intersects the cubic in two points (x_1, y_1) and (x_1, y_2). Now to find the third point (x_3, y_3), substitute the equation of line in the given cubic equation to get:

$$(\lambda x + \nu)^2 = x^3 + ax^2 + bx + c$$

Simplify to get:

$$\Rightarrow x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = 0$$

Now x_1, x_2, x_3 are roots of this equation, and their sum is equal to negative of coefficient of x^2:

$$\Rightarrow x_3 = \lambda^2 - a - x_1 - x_2$$

Substituting this in equation of line we get:

$$\Rightarrow y_3 = \lambda x_3 + \nu$$

(iv) In the formula derived above slope of line at a given point is used instead of two point form, thus replacing:

$$\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y} = \frac{3x^2 + 2ax + b}{2y}$$

we get desired result.

□

Theorem 1.8.2 (Points of Order[22] Two and Three)**.** *Let C be the non-singular cubic curve:*

$$C : y^2 = f(x) = x^3 + ax^2 + bx + c$$

(i) A point $P = (x, y) \neq \mathcal{O}$ on C has order two if and only if $y = 0$.

(ii) C has exactly four points of order 2. These four points form a group which is a product of two cyclic groups of order two.

(iii) A point $P = (x, y) \neq \mathcal{O}$ on C has order three if and only if x is a root of polynomial:

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2)$$

(iv) C has exactly nine points of order dividing 3. These nine points form a group which is product of two cyclic groups of order three.

Proof. (i) We need to find points in our group which satisfy $2p = \mathcal{O}$, but $P \neq \mathcal{O}$. Instead of $2p = \mathcal{O}$ it is easier to look at equivalent condition $P = -P$.
Since in our group, $-(x, y) = (x, -y)$ [reflection about x axis], these are the points with $y = 0$:

$$P_1 = (\alpha_1, 0), \qquad P_2 = (\alpha_2, 0), \qquad P_3 = (\alpha_3, 0)$$

where $\alpha_1, \alpha_2, \alpha_3$ are roots of given cubic polynomial $f(x)$.
If we allow complex coordinates, there are exactly three points of order 2, because non-singularity of curve ensures that $f(x)$ has distinct roots.

(ii) If we take all points satisfying $2p = \mathcal{O}$, including $\mathcal{O}$, then we get the set $\{\mathcal{O}.P_1, P_2, P_3\}$.
Since group of rational points on elliptic curve is abelian, the set of solutions of $2P = \mathcal{O}$ forms a subgroup. So we have a group of order 4. Since every element has order one or two, it is obvious that this group is a Four Group[23], a direct product of two groups of order two.

(iii) Again instead of $3P = \mathcal{O}$ we will look at $2P = -P$. Now if we denote the x coordinate of point P by $x(P)$ then, a point of order 3 must satisfy: $x(2P) = x(-P) = x(P)$. Since $P \neq \mathcal{O}$, we get: $2P = \pm P$, so either $P = \mathcal{O}$ or $3P = \mathcal{O}$. But since it is given that $P \neq \mathcal{O}$ only possibility is $3P = \mathcal{O}$. Thus the points of order 3 are the points satisfying $x(2P) = x(P)$, now using our duplication formula:

$$x = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$$

Now cross multiply and rearrange terms to get:

$$3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2) = 0$$

Thus x is root of $\psi_3(x)$.

(iv) Observe that:

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = \frac{(x^3 + 2ax + b)^2}{4(x^3 + ax^2 + bx + c)} - a - 2x = \frac{\big(f'(x)\big)^2}{4f(x)} - a - 2x$$

Thus, we can rewrite $\psi_3(x)$ as:

$$\psi_3 = 2(6x + 2a)f(x) - \big(f'(x)\big)^2 = 2f(x)f''(x) - \big(f'(x)\big)^2$$

---

[22] An element P of any group is said to have order m if: $mP = \underbrace{P + \ldots + P}_{\text{m summands}} = \mathcal{O}$, but $m'P \neq \mathcal{O}$ for all integers $1 \leq m' < m$.

[23] The Klein four group (Viergruppe), V_4, is the group of order 4 and multiplication table:

$*$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

.

It is abelian and the simplest group which is not cyclic.

Now we claim that $\psi_3(x)$ has four distinct (complex) roots since $\psi_3(x)$ and $\psi_3'(x)$ have no common roots. Because if

$$\psi_3'(x) = 2f(x)f'''(x) = 2f(x) \times 6 = 12f(x)$$

and $\psi_3(x)$ has a common root, then $f(x)$ and $f'(x)$ should also have a common root, but since C is non-singular, $f(x)$ and $f'(x)$ have no common root. Hence our claim is true.
Let, $\beta_1, \beta_2, \beta_3, \beta_4$ be the four complex roots of $\psi_3(x)$ and for each β_i, let $\delta_i = \sqrt{f(\beta_i)}$. Then as proved in last part, the set:

$$\{(\beta_1, -\delta_1), (\beta_2, -\delta_2), (\beta_3, -\delta_3), (\beta_4, -\delta_4), (\beta_1, \delta_1), (\beta_2, \delta_2), (\beta_3, \delta_3), (\beta_4, \delta_4)\}$$

is the complete set of distinct points of order 3 on C.
Also, $\delta_i \neq 0$, otherwise the point will be of order 2, contradicting the fact that the point is of order 3. The only other point on C with order dividing 3 is the point of order one, namely $\mathcal{O}$. Thus, C has exactly nine points of order dividing 3.
Note that there is only one (abelian) group with nine elements such that every element has order dividing 3, namely the product of two cyclic groups of order 3.

☐

Remark: Geometrically the points of order 3 are points of inflection of our elliptic curve.

A method of changing coordinates to move point at infinity to a finite place

Recall that we converted any cubic to Weierstrass form by doing a set of *rational transformations*, now we will convert the curve in Weierstrass form to another form, where the point at infinity will be at finite place. Consider the curve:

$$y^2 = x^3 + ax^2 + bx + c$$

Now, substitute:

$$x = \frac{t}{s} \qquad \text{and} \qquad y = \frac{1}{s}$$

to get our new equation:

$$s = t^3 + at^2s + bts^2 + cs^3$$

Now this curve when plotted in ts plane, have all points of old xy plane except the points where $y = 0$, and zero element of our curve $\mathcal{O}$ is now at origin $(0, 0)$ in ts plane.

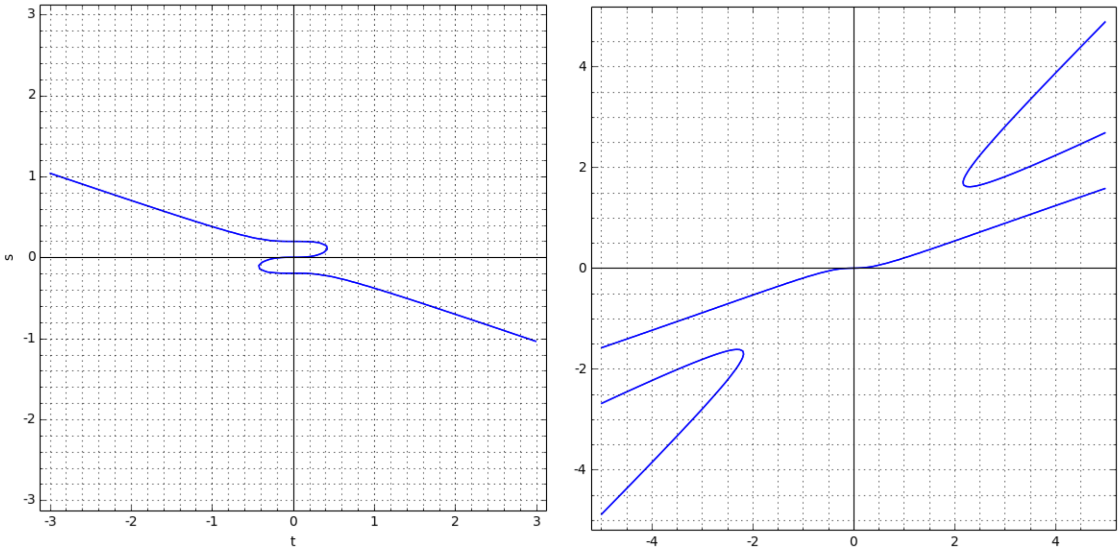

Figure 1.2: ILLUSTRATION: Here I have transformed the curves shown in Figure 1.1, equation of the curve on left and right hand side transforms to: $s = t^3 + 25s^3$ and $s = t^3 - 6t^2s + 11ts^2 - 6s^3$ respectively. [Curves plotted using SageMath Version 6.6]

Also, a line $y = \lambda x + \nu$ in the (x, y) plane corresponds to a line in the (t, s) plane. If we divide $y = \lambda x + \nu$ by νy, we get:

$$s = -\frac{\lambda}{\nu}t + \frac{1}{\nu}$$

Thus we can add points in (t, s) plane by same procedure as in (x, y) plane.

Theorem 1.8.3. *Let C be a non-singular cubic curve:*

$$C : y^2 = f(x) = x^3 + ax^2 + bx + c$$

Now, let p be a prime, R the ring[24] *of rational numbers with denominator prime to p, and let $C(p^\Omega)$ be the set of rational points (x, y) on our curve for which x has a denominator divisible by $p^{2\Omega}$, plus the point $\mathcal{O}$.*

(i) $C(p)$ consists of all rational points $(x, y)$for which the denominator of either x or y is divisible by p.

(ii) For every $\Omega \geq 1$, the set $C(p^\Omega)$ is a subgroup of group of rational points $C(\mathbb{Q})$.

(iii) The map:

$$\frac{C(p^\Omega)}{C(p^{3\Omega})} \longrightarrow \frac{p^\Omega R}{p^{3\Omega}R}$$

$$P = (x, y) \longmapsto t(P) = \frac{x}{y}$$

is a one-to-one homomorphism[25]*. (By convention, $\mathcal{O} \mapsto 0$).*

(iv) For every prime p, the subgroup $C(p)$ contains no points of finite order (other than $\mathcal{O}$).

Proof. (i) Put $\Omega = 1$ to get desired result. Since a number divisible by p^2 is also divisible by p.

(ii) Let's look at the divisibility of new coordinates (s, t), described above, by powers of p. Let (x, y) be a rational point of our curve in the xy plane lying in $C(p^\Omega)$. Since every non-zero rational number can be written in the form $\frac{m}{n}p^\Omega$, where m, n are integers prime to p, $n > 0$, and the fraction $\frac{m}{n}$ is in lowest form. We define the *power* of such a rational number to be the integer Ω, and write:

$$\text{pow}\left(\frac{m}{n}p^\Omega\right) = \Omega$$

Consider a point (x, y) on given cubic curve, where p divides the denominator of x, say:

$$x = \frac{m}{np^\mu} \quad \text{and} \quad y = \frac{u}{wp^\sigma}$$

where $\mu > 0$ and p does not divide m, n, u, w. Now substitute this value of point in equation of curve:

$$\frac{u^2}{w^2p^{2\sigma}} = \frac{m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}}$$

Since $p \not| u^2$ and $p \not| w^2$, so

$$\text{pow}\left(\frac{u^2}{w^2p^{2\sigma}}\right) = -2\sigma$$

Also, $\mu > 0$ and $p \not| m$, it follows that:

$$p \not|(m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu})$$

hence:

$$\text{pow}\left(\frac{m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}}\right) = -3\mu$$

---

[24] It is a beautiful ring in the sense that it has unique unique factorization and it has only one prime, the prime p. The units of R are just the rational numbers with numerator and denominator prime to p.

[25] A mapping from one algebraic system to a like algebraic system which preserves structure.

Thus, $2\sigma = 3\mu$.
In particular, $\sigma > 0$, ad so p divides the denominator of y. Further, the relation $2\sigma = 3\mu$, means that $2|\mu$ and $3|\sigma$, so we have $\mu = 2\Omega$ and $\sigma = 3\Omega$ for some integer $\Omega > 0$. Similar result will be obtained when we assume that p divides the denominator of y.
Thus we can write given condition of $C(p^\Omega)$ as:

$$C(p^\Omega) = \{(x, y) \in C(\mathbb{Q}) : \text{pow}(x) \leq -2\Omega \quad \text{and} \quad \text{pow}(y) \leq -3\Omega\}$$

Thus,

$$C(\mathbb{Q}) \supset C(p) \supset C(p^2) \supset C(p^3) \supset \dots$$

By convention we will also include the zero element $\mathcal{O}$ in $C(p^\Omega)$.
So we can write:

$$x = \frac{m}{np^{2(\Omega+i)}} \qquad \text{and} \qquad y = \frac{u}{wp^{3(\Omega+i)}}$$

for some $i \geq 0$. Then:

$$t = \frac{x}{y} = \frac{mw}{nu} p^{\Omega+i} \qquad \text{and} \qquad s = \frac{1}{y} = \frac{w}{u} p^{3(\Omega+i)}$$

Thus our point (t, s) is in $C(p^\Omega)$ if and only if $t \in p^\Omega R$ and $s \in p^{3\Omega} R$. This means that p^Ω divides the numerator of t and $p^{3\Omega}$ divides numerator of s.
Now to prove given statement, we have to add points and show that if a high power of p divides the t coordinate of two points, then the same power of p divides the t coordinate of their sum.
If, given to us are points $P_1 = (t_1, s_1)$ and $P_2 = (t_2, s_2)$, we need to find coordinates of $P_1 * P_2 = P_3 = (t_3, s_3)$, following same method as in Theorem 1.8.1[26], we get:

$$t_3 = -\frac{\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3} - t_1 - t_2 \quad \text{and} \quad s_3 = \alpha t_3 + \beta$$

where,

$$\alpha = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_2 + t_1)s_2 + bs_2^2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)} \quad \text{and} \quad \beta = s_1 - \alpha t_1 = s_2 - \alpha t_2$$

Note that, if $P_1 = P_2$, then substitute $t_2 = t_1$ and our above formula still works (duplication formula).
Now to find $P_1 + P_2$, we draw the line through (t_3, s_3) and the zero element $(0, 0)$, and take the third intersection with the curve. Clearly, the third point of intersection will be $(-t_3, -s_3)$.
Observe that the numerator of α lies in $p^{2\Omega} R$, because each of t_1, s_1, t_2, s_2 is in $p^\Omega R$ [since $C(p^\Omega) \supset C(p^{3\Omega})$]. For the same reason, the quantity $-at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)$ is in $p^{2\Omega} R$, so the denominator in α is a unit in R. *This all has been possible due to presence of 1 in denominator.* It follows that $\alpha \in p^{2\Omega} R$.
Since, $s_1 \in p^{3\Omega} R$ and $\alpha \in p^{2\Omega} R$, and $t_1 \in p^\Omega R$, it follows from the formula, $\beta = s_1 - \alpha t_1$, that $\beta \in p^{3\Omega} R$. Further, since denominator of t_3 is also a unit in R. Looking at expression for $t_1 + t_2 + t_3$ in formula for t_3 we get:

$$t_1 + t_2 + t_3 \in p^{3\Omega} R \in p^\Omega R$$

Since, $t_1, t_2 \in p^\Omega R$, it follows that $t_3 \in p^\Omega R$, and so $-t_3 \in p^\Omega R$.
This proves that if t coordinates of P_1 and P_2 lie in $p^\Omega R$, then t coordinates of $P_1 + P_2$ also lies in $p^\Omega R$, Further, if the t coordinate of $P = (t, s)$ lies in $p^\Omega R$, then it is clear that t coordinate of $-P = (-t, -s)$ also lies in $p^\Omega R$. This shows that $C(p^\Omega)$ is closed under addition and taking negatives; hence it is a subgroup of $C(\mathbb{Q})$.

(iii) In last part we have proven something a bit stronger, if $P_1, P_2 \in C(P^\Omega)$, then:

$$t(P_1) + t(P_2) - t(P_1 + P_2) \in p^{3\Omega} R$$

where $t(P)$ denotes the t coordinate of point P.
This last formula tells us more than the mere fact that $C(P^\Omega)$ is a subgroup. We can rewrite above equation as:

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \pmod{p^{3\Omega} R}$$

---

[26] For full calculations refer pp. 52-53 of [10]

Note that the + in $t(P_1+P_2)$ indicates addition on cubic curve, where as + in $t(P_1)+t(P_2)$ is addition in R, which is just addition of rational numbers.
So the map, $P \mapsto t(P)$, is a not an homomorphism from $C(p^\Omega)$ into the additive group of rational numbers because they are equivalent but *not* equal.
But we get a homomorphism from $C(p^\Omega)$ to quotient group $\dfrac{p^\Omega R}{p^{3\Omega}R}$, by sending P to $t(P)$; and kernel of this homomorphism consists of all points P with $t(P) \in p^{3\Omega}R$. Thus, the kernel is just $C(p^{3\Omega})$, so we obtain the one-to-one homomorphism,

$$\frac{C(p^\Omega)}{C(p^{3\Omega})} \longrightarrow \frac{p^\Omega R}{p^{3\Omega}R}$$

$$P = (x,y) \longmapsto t(P) = \frac{x}{y}$$

(iv) Let the order of P be m. Since $P \neq \mathcal{O}$, we know $m \neq 1$. Consider any prime p. Suppose, $P \in C(p)$ The point $P = (x,y)$ may be contained in a smaller group $C(p^\Omega)$ but it can't be contained in all of the groups $C(p^\Omega)$ because the denominator of x can't be divisible by arbitrarily high powers of p. So we can find some $\Omega > 0$, such that, $P \in C(p^\Omega)$, but $P \notin C(p^{\Omega+1})$.
Now consider two cases:

Case 1: $p \not| m$
Using the congruence relation derived in previous part again and again we will get,

$$t(mP) \equiv mt(P) \pmod{p^{3\Omega}R}$$

Since, $mP = \mathcal{O}$, we have $t(mP) = t(\mathcal{O}) = 0$. On the other hand, since m is prime to p, it is a unit in R. Therefore,

$$0 \equiv t(P) \pmod{p^{3\Omega}R}$$

This means that $P \in C(p^{3\Omega})$, contradicting the fact that, $P \notin C(p^{\Omega+1})$.

Case 2: $p|m$
Let, $m = pn$, and look at point $P' = nP$. Since P has order m, it is clear that P' has order $m/n = p$. Further, since $P \in C(p)$ and $C(p)$ is a subgroup, we see that $P' \in C(p)$. As above,

$$0 \equiv pt(P') \pmod{p^{3\Omega}R}$$

$$\Rightarrow t(P') \equiv 0 \pmod{p^{3\Omega-1}R}$$

Since, $3\Omega - 1 \geq \Omega + 1$, we again get a contradiction to fact that $P' \notin C(p^{\Omega+1})$.

Combining both cases we complete our proof.

□

Theorem 1.8.4 (Nagell-Lutz Theorem). *Let C be a non-singular cubic curve:*

$$C : y^2 = f(x) = x^3 + ax^2 + bx + c$$

with integer coefficients a, b, c; let D be the discriminant[27] *of the cubic polynomial $f(x)$,*

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

Let $P = (x,y)$ be a rational point of finite order. Then x, y are integers and either $y = 0$, in which case P has order two, or else y divides D.

Proof. We will divide proof in two parts (first one is difficult and second one is easy):

Part 1: *Let $P = (x,y) \neq \mathcal{O}$ be a rational point of finite order. Then x and y are integers.*

If $P = (x,y)$ is a point of finite order, then from Theorem 1.8.3, we know that $P \notin C(p)$ for all primes p. This means that the denominators of x and y are divisible by no primes, hence x and y are integers.

---

[27] If we factor f over the complex numbers, $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, then $D = (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2$ so the non-vanishing of D implies that the roots of $f(x)$ are distinct.

Part 2: *Let $P = (x, y)$ be a point on our cubic curve such that both P and $2P$ have integer coordinates. Then either $y = 0$ or $y \big| D$.*

If P has order 2, we know that in this case, $y = 0$ and we are done.
Let $y \neq 0$. Then, $2P \neq \mathcal{O}$, from previous theorem. Write $2P = (X, Y)$. By assumption, x, y, X, Y are all integers. As per duplication formula:

$$X = \frac{\big(f'(x)\big)^2}{4y^2} - a - 2x$$

Since x, X, a all are integers, it follows that,

$$4y^2 \Big| \big(f'(x)\big)^2 \quad \Rightarrow y \big| f'(x) \tag{1.11}$$

But,

$$y^2 = f(x) \quad \Rightarrow y \big| f(x) \tag{1.12}$$

Now from general theorem of discriminants, for $f(x) = x^3 + ax^2 + bx + c$, we get:

$$D = [(18b - 6a^2)x - (4a^3 - 15ab + 27c)]f(x) + [(2a^2 - 6b^2)x^2 + (2a^3 - 7ab + 9c)x + (a^2b + 3ac - 4b^2)]f'(x)$$

Thus, there are polynomials $r(x)$ and $s(x)$ with integer coefficients so that D can be written as:

$$D = r(x)f(x) + s(x)f'(x)$$

Now, since the coefficients of $r(x)$ and $s(x)$ are integers, these functions also take on integer values when evaluated at an integer x.
Thus from (1.11) and (1.12) it follows that $y \big| D$.

□

Remark: A consequence of this theorem is that a cubic curve has only a finite number of rational points of finite order.

Definition 1.8.18 (Height)**.** Let, $x = \dfrac{m}{n}$ be a rational number written in lowest terms. Then, the height $H(x)$ is defined as maximum of the absolute values of the numerator and the denominator.

$$H(x) = H\left(\frac{m}{n}\right) = \max\{|m|, |n|\}$$

Definition 1.8.19 (Height of a point)**.** If, $y^2 = f(x) = x^3 + ax^2 + bx + c$ is a non-singular cubic curve with integer coefficients a, b, c, and if $P = (x, y)$ is a rational point on the curve, then *height of* P is simply height of its x coordinate.

$$H(P) = H(x)$$

For the point at infinity, $\mathcal{O}$, $H(\mathcal{O}) = 1$.

Definition 1.8.20 (Height Logarithm)**.** *Height logarithm* is a non-negative number defined as logarithm of height of a point.

$$h(P) = \log H(P)$$

Hence for the point at infinity, $\mathcal{O}$, $h(\mathcal{O}) = 0$.

Theorem 1.8.5. *Let C and $\overline{C}$ be the elliptic curves, given by the equations:*

$$C : y^2 = x^3 + ax^2 + bx \qquad \text{and} \qquad \overline{C} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x$$

where, $\overline{a} = -2a$ and $\overline{b} = a^2 - 4b$. Let $T = (0, 0) \in C$.

(i) There is a homomorphism $\phi : C \to \overline{C}$ defined by:

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right), & \text{if} \quad P = (x, y) \neq \mathcal{O}, T \\ \overline{\mathcal{O}}, & \text{if} \quad P = \mathcal{O} \quad \text{or} \quad P = T \end{cases}$$

The kernel of ϕ is $\{\mathcal{O}, T\}$.

(ii) Applying the same process to $\overline{C}$ gives a map $\overline{\phi} : \overline{C} \to \overline{\overline{C}}$. Where:

$$\overline{\overline{C}} : y^2 = x^3 + \overline{\overline{a}}x^2 + \overline{\overline{b}}x$$

The curve $\overline{\overline{C}}$ is isomorphic to C via map $(x, y) \to (x/4, y/8)$.
There is thus a homomorphism $\psi : \overline{C} \to C$ defined by:

$$\psi(\overline{P}) = \begin{cases} \left(\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}(\overline{x}^2 - \overline{b})}{8\overline{x}^2}\right), & \text{if} \quad \overline{P} = (\overline{x}, \overline{y}) \neq \overline{\mathcal{O}}, \overline{T} \\ \mathcal{O}, & \text{if} \quad \overline{P} = \overline{\mathcal{O}} \quad \text{or} \quad \overline{P} = \overline{T} \end{cases}$$

The composition $\psi \circ \phi : C \to C$ is multiplication by two: $(\psi \circ \phi)(P) = 2P$.

(iii) If we apply the map ϕ to rational points Γ, we get a subgroup of the set of rational points $\overline{\Gamma}$, we denote this subgroup by $\phi(\Gamma)$, and call it the image of Γ by ϕ. Then:

- *(a) $\overline{\mathcal{O}} \in \phi(\Gamma)$*
- *(b) $\overline{T} = (0, 0) \in \phi(\Gamma)$ if and only if $\overline{b} = a^2 - 4b$ is a perfect square.*
- *(c) Let $\overline{P} = (\overline{x}, \overline{y}) \in \overline{\Gamma}$ with $\overline{x} \neq 0$. Then $\overline{P} \in \phi(\Gamma)$ if and only if $\overline{x}$ is the square of a rational number.*

Sketch of Proof. (i) Firstly check that, ϕ maps points of C to points of $\overline{C}$, by replacing the values of $\overline{x}$ in the equation of $\overline{C}$. To prove this is a homomorphism, we need to prove that $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2)$ for all $P_1, P_2 \in C$. [Note that the first plus sign is addition on C, whereas the second one is addition on $\overline{C}$.] Make different cases like,

- (a) P_1 or P_1 is $\mathcal{O}$ [trivial]
- (b) P_1 or P_2 is T [use explicit formula from addition law]
- (c) $P_1 + P_2 + P_3 = \mathcal{O}$, then $\phi(P_1) + \phi(P_2) + \phi(P_3) = \overline{\mathcal{O}}$ [observe that ϕ takes negatives to negatives and this statement is equivalent to proving P_1, P_2, P_3 are collinear]

(ii) Note that $\overline{\overline{a}} = -2\overline{a} = 4a$ and $\overline{\overline{b}} = \overline{a}^2 - 4\overline{b} = 16b$, thus:

$$\overline{\overline{C}} : y^2 = x^3 + 4ax^2 + 16bx$$

Hence it is clear the the map, $(x, y) \to (x/4, y/8)$ is an isomorphism from $\overline{C}$ to C. Since the map $\psi : \overline{C} \to C$ is the composition of $\overline{\phi} : \overline{C} \to \overline{\overline{C}}$ with the isomorphism $\overline{\overline{C}} \to C$, we get that ψ is a well defined homomorphism from $\overline{C}$ to C.
To verify that $\psi \circ \phi$ is multiplication by two, use the duplication formula derived earlier, to get: $(\psi \circ \phi)(x, y) = 2(x, y)$ and $(\phi \circ \psi)(\overline{x}, \overline{y}) = 2(\overline{x}, \overline{y})$. And then check that $(\psi \circ \phi)(P) = \mathcal{O}$ in the cases that P is a point of order two [our duplication formula won't work here, since $x = y = 0$ in this case.]

(iii)

- (a) $\overline{\mathcal{O}} = \phi(\mathcal{O})$ [trivial]
- (b) From formula for ϕ, $\overline{T} \in \phi(\Gamma)$ if and only if there is a rational point $(x, y) \in \Gamma$ such that $\frac{y^2}{x^2} = 0, x \neq 0$ [because then, $\phi(T) = \mathcal{O}$ not $\overline{T}$]. Thus put $y = 0$ in the equation of Γ.
- (c) If $(\overline{x}, \overline{y}) \in \phi(\Gamma)$ is a point with $\overline{x} \neq 0$ then the defining formula for ϕ shows that $\overline{x} = \frac{y^2}{x^2}$ is a square of a rational number. Suppose conversely that $\overline{x} = w^2$ for some rational number w. Now we have to find a rational point on C that maps to $(\overline{x}, \overline{y})$.
  The homomorphism ϕ has two elements in its kernel, $\mathcal{O}$ and T. Thus if $(\overline{x}, \overline{y})$ lies in $\phi(\Gamma)$, there will be two points of Γ that map to it. Let: $x_1 = \frac{1}{2}\left(w^2 - a + \frac{\overline{y}}{w}\right), y_1 = x_1 w$ and $x_2 = \frac{1}{2}\left(w^2 - a - \frac{\overline{y}}{w}\right), y_2 = -x_2 w$. Then verify that the points $P_i = (x_i, y_i)$ are on C, and that $\phi(P_i) = (\overline{x}, \overline{y})$ for $i = 1, 2$. Since P_1 and P_2 are rational points this will prove that $(\overline{x}, \overline{y}) \in \phi(\Gamma)$

Theorem 1.8.6 (Mordell's Theorem for curves with a Rational Point of Order Two)**.** *Let C be a non-singular cubic curve given by equation:*

$$C : y^2 = f(x) = x^3 + ax^2 + bx$$

where a, b are integers. Then group of rational points $C(\mathbb{Q})$ is a finitely generated abelian group.

Proof. Firstly, to ease notation let, $\Gamma = C(\mathbb{Q})$. We will divide the proof of this theorem into 5 parts.

Part 1: *For every real number M, the set $\{P \in \Gamma : h(P) \leq M\}$ is finite.*

Consider point, $P = (x, y)$, now, $H(P) = H(x)$. Let, $x = \dfrac{m}{n}$, so, $H(P) = \max\{|m|, |n|\}$. Now if the height of P is less than some fixed constant, say M', then both $|m|$ and $|n|$ are less than that finite constant, so there are only finitely many possibilities for m and n. Thus the set $\{P \in \Gamma : H(P) \leq M'\}$ is finite. Since, $h(P) = \log H(P)$, the same will hold if we use $h(P)$ in place of $H(P)$. Hence the set $\{P \in \Gamma : h(P) \leq M\}$ is finite, for given fixed constant M.

Part 2: *Let P_0 be a fixed rational point on C. There is a constant ε_0 depending on P_0 and on a, b, so that $h(P + P_0) \leq 2h(P) + \varepsilon_0$ for all $P \in \Gamma$*

This is trivial if $P_0 = \mathcal{O}$; so let, $P_0 = (x_0, y_0) \neq \mathcal{O}$. To prove existence of ε_0 it is enough to prove that the inequality holds for all P except those in some fixed finite set. This is true because, for nay finite number P, we just look at the differences $h(P + P_0) - h(P)$ and take ε_0 larger than the finite number of values that occur. Thus we will prove this proposition for $P \notin \{P_0, -P_0, \mathcal{O}\}$, since if $P = (x, y)$ and $x = x_0$ which you can prove using duplication formula and repeating same argument.
Let, $P = (x, y)$ and $x \neq x_0$. We can write:

$$P + P_0 = P' = (\delta, \eta)$$

Now, $h(P + P_0) = h(\delta)$, from addition formula derived in Theorem 1.8.1 (with $c = 0$),

$$\delta = \lambda^2 - a - x - x_0 \qquad \text{where} \quad \lambda = \frac{y - y_0}{x - x_0}$$

$$\Rightarrow \delta = \frac{(y - y_0)^2 - (x - x_0)^2(x + x_0 + a)}{(x - x_0)^2}$$

$$\Rightarrow \delta = \frac{(y^2 - x^3) + (-2y_0)y + (x_0 - a)x^2 + (x_0^2 + 2ax_0)x + (y_0^2 - ax_0^2 - x_0^3)}{x^2 + (-2x_0)x + x_0^2}$$

But, $y^2 - x^3 = ax^2 + bx$, thus for some integers, A, B, C, D, E, F, G we can rewrite above statement as:

$$\Rightarrow \delta = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G} \tag{1.13}$$

Thus, we have integers A, B, C, D, E, F, G, which depend only on a, b, x_0, y_0. Once the curve and the point P_0 are fixed, then the expression is correct fol all points $P \notin \{P_0, -P_0, \mathcal{O}\}$. So it will be all right for our constant ε_0 to depend on A, B, C, D, E, F, G as long as it doesn't depend on (x, y).
Now, if $P = (x, y)$ is a rational point on our curve then suppose we write:

$$x = \frac{m}{M} \qquad \text{and} \qquad y = \frac{n}{N}$$

in lowest terms with $M > 0$ and $N < 0$. Substituting these into the equation of curve, we get:

$$\Rightarrow \frac{n^2}{N^2} = \frac{m^3}{M^3} + a\frac{m^2}{M^2} + b\frac{m}{M}$$

$$\Rightarrow M^3n^2 = N^2m^3 + aN^2Mm^2 + bN^2M^2m$$

Since, N^2 is a factor of all terms on the right hand side, we see that $N^2|M^3n^2$, but $\gcd(n, N) = 1$, so $N^2|M^3$.
Also, $M|N^2m^3$ since it occurs in all factors of right hand side, and since $\gcd(m, M) = 1$, we find $M|N^2$. Using this fact again in the equation obtained above, we find that $M^2|N^2m^3$, so $M|N$. Finally using above equation again, we get, $M^3|N^2m^3$, so $M^3|N^2$.
Thus we have shown that, $N^2|M^3$ and $M^3|N^2$, so $M^3 = N^2$. Further, we also showed that $M|N$, thus if we let $e = \dfrac{N}{M}$ and we use it in $M^3 = N^2$, we get:

$$e^2 = M \qquad \text{and} \qquad e^3 = N$$

Therefore,

$$x = \frac{m}{e^2} \qquad \text{and} \qquad y = \frac{n}{e^3}$$

Now substitute this value on x, y in (1.13), we get:

$$\Rightarrow \delta = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}$$

Thus we have an expression for δ as an integer divided by an integer. We don't know that it is in lowest terms, but cancellation will only make the height smaller. Thus,

$$H(\delta) \leq \max\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\} \tag{1.14}$$

Further, since now, $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$, then the height of P is the maximum of $|m|$ and e^2. In particular,

$$\begin{cases} |m| \leq H(P) \\ e^2 \leq H(P) \quad \Rightarrow e \leq [H(P)]^{1/2} \end{cases} \tag{1.15}$$

. But these coordinate of P also satisfy the equation of given curve, so:

$$n^2 = m^3 + ae^2m^2 + be^4m$$

Now take absolute values and apply triangle inequality to get:

$$|n^2| \leq |m^3| + |ae^2m^2| + |be^4m| \leq [H(P)]^3 + |a|[H(P)]^3 + |b|[H(P)]^3$$

so, if we take $k = \sqrt{1 + |a| + |b|}$, we get:

$$|n| \leq k[H(P)]^{3/2} \tag{1.16}$$

Now using (1.15) and (1.16) in (1.14) and applying triangle inequality we get:

$$\begin{cases} |Ane + Bm^2 + Cme^2 + De^4| \leq \Big(|Ak| + |B| + |C| + |D|\Big)[H(P)]^2 \\ \\ |Em^2 + Fme^2 + Ge^4| \leq \Big(|E| + |F| + |G|\Big)[H(P)]^2 \end{cases}$$

Therefore,

$$H(P + P_0) = H(\delta) \leq \max\Big\{\Big(|Ak| + |B| + |C| + |D|\Big), \Big(|E| + |F| + |G|\Big)\Big\}[H(P)]^2$$

Taking logarithms on both sides gives:

$$h(P + P_0) \leq 2h(P) + \log\left(\max\Big\{\Big(|Ak| + |B| + |C| + |D|\Big), \Big(|E| + |F| + |G|\Big)\Big\}\right)$$

Let, $\varepsilon_0 = \log\left(\max\Big\{\Big(|Ak|+|B|+|C|+|D|\Big), \Big(|E|+|F|+|G|\Big)\Big\}\right)$. Thus, ε_0 depends only on a, b, x_0, y_0 and does not depend on $P = (x, y)$, thus we get:

$$h(P + P_0) \leq 2h(P) + \varepsilon_0$$

Part 3: *There is a constant ε, depending on a, b so that $h(2P) \geq 4h(P) - \varepsilon$ for all $P \in \Gamma$.*

Let $P = (x, y)$, and write $2P = (\delta, \eta)$. Then by duplication formula derived in Theorem 1.8.1 (with $c = 0$) we get:

$$\delta = \lambda^2 - a - 2x \qquad \text{where} \quad \lambda = \frac{f'(x)}{2y}$$

Using $f(x) = y^2$, we get:

$$\delta = \frac{\Big(f'(x)\Big)^2 - (8x + 4a)f(x)}{4f(x)} = \frac{x^4 - 2bx^2 + b^2}{4x^3 + 4ax^2 + 4bx}$$

Note that just as done in our proof of Part - 2, above, it is all right to ignore any finite set of points, since we can always ε larger than $4h(P)$ for all points in that finite set. So we will discard the finitely many points of order 2, i.e. satisfying $2P = \mathcal{O}$. Thus $f(x) \neq 0$ because $2P \neq \mathcal{O}$.
Thus δ is the quotient of two polynomials in x with integer coefficients. Since the cubic $y^2 = f(x)$ is non-singular by assumption, we know that $f(x)$ and $f'(x)$ have no common (complex) roots. Thus, the polynomials in numerator and denominator have no common roots.
Since, $h(P) = h(x)$ and $h(2P) = h(\delta)$. Let, $\delta = \dfrac{\Phi(x)}{\Psi(x)}$, where,

$$\Phi(x) = x^4 - 2bx^2 + b^2 \qquad \text{and} \qquad \Psi(x) = 4x^3 + 4ax^2 + 4bx$$

Thus,

$$h(2P) = \log\Big(max\{|\Phi(x)|, |\Psi(x)|\}\Big)$$

Hence what we have prove is:

$$4h(x) - \varepsilon \leq h\bigg(\frac{\Phi(x)}{\Psi(x)}\bigg)$$

Now, $\Phi(x)$ and $\Psi(x)$ are polynomials with integer coefficients and no common (complex) roots. Also, the maximum of the degrees of Φ and Ψ is 4. Now we will prove two propositions[28]

Proposition 1: *There is an integer $\Lambda \geq 1$, depending on Φ and Ψ, so that for all rational numbers $\dfrac{m}{n}$, the gcd $\bigg(n^4\Phi\Big(\dfrac{m}{n}\Big), n^4\Psi\Big(\dfrac{m}{n}\Big)\bigg)$ divides Λ.*

Firstly, observe that since $\Phi(x)$ and $\Psi(x)$ have no common roots, they are relatively prime in Euclidean ring $\mathbb{Q}[x]$. Thus we can apply Euclidean algorithm to compute, polynomials with rational coefficients, $F(x)$ and $G(x)$, such that,

$$F(x)\Phi(x) + G(x)\Psi(x) = 1 \tag{1.17}$$

Now, we apply Euclid's division algorithm to get:

$$x^4 - 2bx^2 + b^2 = (4x^3 + 4ax^2 + 4bx)\left(\frac{x-a}{4}\right) + \Big((a^2 - 3b)x^2 + abx + b^2\Big)$$

$$4x^3{+}4ax^2{+}4bx = \Big((a^2{-}3b)x^2{+}abx{+}b^2\Big)\left(\frac{4(a^2-3b)x - 4a(a^2-4b)}{(a^2-3b)^2}\right){+}\left(\frac{12b^2(4b-a^2)}{(a^2-3b)^2}x{+}\frac{4ab^2(4b-a^2)}{(a^2-3b)^2}\right)$$

$$(a^2{-}3b)x^2{+}abx{+}b^2 = \left(\frac{4b^2(4b-a^2)(3x+a)}{(a^2-3b)^2}\right)\left(\frac{(a^2-3b)^2\big(3(a^2-3b)x + (6b-a^2)a\big)}{36b^2(4b-a^2)}\right){+}\frac{a^4 - 6a^2b + 9b^2}{9}$$

Now following the Remainder Substitution & Isolation method, that we follow to solve linear diophantine equation, [Section 2.1.1], we get:

$$\frac{a^4 - 6a^2b + 9b^2}{9} = \left(\Phi(x) - \Psi(x)\left(\frac{x-a}{4}\right)\right) - \left(\Psi(x) - \left(\Phi(x) - \Psi(x)\left(\frac{x-a}{4}\right)\right)P(x)Q(x)\right)$$

where,

$$P(x) = \left(\frac{4(a^2-3b)x - 4a(a^2-4b)}{(a^2-3b)^2}\right)$$

$$Q(x) = \frac{(a^2-3b)^2\big(3(a^2-3b)x + (6b-a^2)a\big)}{36b^2(4b-a^2)}$$

---

[28] These propositions are actually true for any such polynomials, for general proof refer pp. 72-75 of [10].

$$\Rightarrow \frac{a^4-6a^2b+9b^2}{9} = \left(\Phi(x)-\Psi(x)\left(\frac{x-a}{4}\right)\right) - \left(\Psi(x)-P(x)Q(x)\Phi(x)+P(x)Q(x)\Psi(x)\left(\frac{x-a}{4}\right)\right)$$

$$\Rightarrow \frac{a^4-6a^2b+9b^2}{9} = \Phi(x)-\Psi(x)\left(\frac{x-a}{4}\right)-\Psi(x)+P(x)Q(x)\Phi(x)-P(x)Q(x)\Psi(x)\left(\frac{x-a}{4}\right)$$

$$\Rightarrow \frac{a^4-6a^2b+9b^2}{9} = \Big(1+P(x)Q(x)\Big)\Phi(x) + \Big(\frac{a-x}{4}\big(1+P(x)Q(x)\big)-1\Big)\Psi(x)$$

Thus we get:

$$\begin{cases} F(x) = \left(1+\left(\frac{4(a^2-3b)x-4a(a^2-4b)}{(a^2-3b)^2}\right)\left(\frac{(a^2-3b)^2\big(3(a^2-3b)x+(6b-a^2)a\big)}{36b^2(4b-a^2)}\right)\right)\dfrac{9}{a^4-6a^2b+9b^2} \\ \\ G(x) = \left(\frac{a-x}{4}\left(1+\left(\frac{4(a^2-3b)x-4a(a^2-4b)}{(a^2-3b)^2}\right)\left(\frac{(a^2-3b)^2\big(3(a^2-3b)x+(6b-a^2)a\big)}{36b^2(4b-a^2)}\right)\right)-1\right)\dfrac{9}{a^4-6a^2b+9b^2} \end{cases}$$

Let A be a large enough integer so that $AF(x)$ and $AG(x)$ have integer coefficients. Further, now 3 is the maximum degree of F and G. Now we will evaluate (1.17) for $x = m/n$:

$$F\left(\frac{m}{n}\right)\Phi\left(\frac{m}{n}\right) + G\left(\frac{m}{n}\right)\Psi\left(\frac{m}{n}\right) = 1$$

Now to make left hand side integer multiply by An^{3+4} on both sides:

$$An^3F\left(\frac{m}{n}\right)n^4\Phi\left(\frac{m}{n}\right) + An^3G\left(\frac{m}{n}\right)n^4\Psi\left(\frac{m}{n}\right) = An^7$$

Note that, $n^4\Phi\left(\frac{m}{n}\right)$ and $n^4\Psi\left(\frac{m}{n}\right)$ are surely integers. So, we can calculate their gcd. Let

$$\gcd\left(n^4\Phi\left(\frac{m}{n}\right), n^4\Psi\left(\frac{m}{n}\right)\right) = \gamma \tag{1.18}$$

Now, since $An^3F\left(\frac{m}{n}\right)$ and $An^3G\left(\frac{m}{n}\right)$ are also integers, so, γ divides the right hand side, thus

$$\gamma \big| An^7 \tag{1.19}$$

But γ should divide one fixed number.
Now, observe that:

$$n^4\Phi\left(\frac{m}{n}\right) = m^4 - 2Abm^2n^2 + Ab^2n^4$$

Now to be able to use, (1.19), we multiply by An^{4+3-1} to get:

$$\Big(An^7\Big)n^3\Phi\left(\frac{m}{n}\right) = Am^4n^6 - 2Abm^2n^8 + Ab^2n^{10} = Am^4n^6 - An^7(2bm^2n) + An^7(b^2n^3)$$

Thus since γ divides left hand side and all quantities are integers, it should also divide right hand side, thus:

$$\gamma \big| Am^4n^6$$

But, m, n are relatively prime, so (1.19) implies that, $\gamma \big| An^6$.
Now repeating this process 6 more times we will get: $\gamma \big| A$, thus proving our proposition.

Proposition 2: *There are constants ε_1 and ε_2, depending on Φ and Ψ, so that for all rational numbers $\frac{m}{n}$ which are not roots of Ψ, $4h\Big(\frac{m}{n}\Big) - \varepsilon_1 \le h\Big(\frac{\Phi(m/n)}{\Psi(m/n)}\Big) \le 4h\Big(\frac{m}{n}\Big) + \varepsilon_2$.*

Here we need to prove two inequalities, upper bound can be proved as in Part - 2 [just need to use duplication formula instead of general formula].
To prove lower bound, as done earlier, we will exclude some finite set of rational numbers. We assume that the rational number $\dfrac{m}{n}$ is not root of $\Phi(x)$. [in starting of proof of this part, we have already excluded all those points for which $\Psi(x) = 4f(x)$ is zero]. If r is any non-zero rational number, it is clear from definition that $h(r) = h\left(\dfrac{1}{r}\right)$. So we can reverse the role of Φ and Ψ if

necessary.
Thus, we can say:

$$\delta = \frac{\Phi\left(\frac{m}{n}\right)}{\Psi\left(\frac{m}{n}\right)} = \frac{n^4\Phi\left(\frac{m}{n}\right)}{n^4\Psi\left(\frac{m}{n}\right)}$$

This gives an expression for δ as a quotient of integers, so:

$$H(\delta) = \max\left\{\left|n^4\Phi\left(\frac{m}{n}\right)\right|, \left|n^4\Psi\left(\frac{m}{n}\right)\right|\right\}$$

except for the possibility that they may have common factors.
We proved in previous proposition that there is some integer, $\Lambda \geq 1$, independent of m and n, so that the greatest common divisor of $n^4\Phi\left(\frac{m}{n}\right)$ and $n^4\Psi\left(\frac{m}{n}\right)$ divides Λ. This bounds possible cancellation, and we find that:

$$H(\delta) \geq \frac{1}{\Lambda}\max\left\{\left|n^4\Phi\left(\frac{m}{n}\right)\right|, \left|n^4\Psi\left(\frac{m}{n}\right)\right|\right\}$$

Since,

$$\max(a, b) = \frac{a+b+|a-b|}{2} \geq \frac{a+b}{2}$$

We get:

$$\Rightarrow H(\delta) \geq \frac{\left|n^4\Phi\left(\frac{m}{n}\right)\right| + \left|n^4\Psi\left(\frac{m}{n}\right)\right|}{2\Lambda}$$

To compare $4h(x)$ and $h(\delta)$ is equivalent to comparing $H(\delta)$ to the quantity $H\left(\frac{m}{n}\right)^4 = \max\{|m|^4, |n|^4\}$, so we consider quotient:

$$\frac{H(\delta)}{H\left(\frac{m}{n}\right)^4} \geq \frac{\left|n^4\Phi\left(\frac{m}{n}\right)\right| + \left|n^4\Psi\left(\frac{m}{n}\right)\right|}{2\Lambda\max\{|m|^4, |n|^4\}}$$

Now, if we substitute back values of functions, we get:

$$\frac{H(\delta)}{H\left(\frac{m}{n}\right)^4} \geq \frac{\left|m^4 - 2bm^2n^2 + b^2n^4\right| + \left|4m^3n + 4am^2n^2 + 4bmn^3\right|}{2\Lambda\max\{|m|^4, |n|^4\}}$$

$$\frac{H(\delta)}{H\left(\frac{m}{n}\right)^4} \geq \frac{\left|m^2 - bn^2\right|^2 + \left|4m^3n + 4am^2n^2 + 4bmn^3\right|}{2\Lambda\max\{|m|^4, |n|^4\}} > 0$$

This quantity is strictly positive, so it must have a positive minimum value, because we have excluded all the points where Φ and Ψ are zero.
Call that minimum value, C , then:

$$\frac{H(\delta)}{H\left(\frac{m}{n}\right)^4} \geq C$$

Taking logarithm both sides:

$$h(\delta) \geq 4H\left(\frac{m}{n}\right) + \log(C)$$

Now, put, $\varepsilon = -\log(C)$, to get desired result.

This completes the proof of this part.

Part 4: *The subgroup* 2Γ *has a finite index*[29] *in* Γ.

In this part we will make use of fact that, given elliptic curve has a rational point of order 2, namely $T = (0, 0)$, since, $2T = \mathcal{O}$. Also since the curve is non-singular, the discriminant, $D = b^2(a^2 - 4b)$ is non-zero. To prove this part firstly we will borrow all the notations from Theorem 1.8.5 (to save

---

[29] Number of distinct right cosets of 2Γ in Γ.

space). Now if we can prove that the index $\big(\overline{\Gamma} : \phi(\Gamma)\big)$ is finite and also the index $\big(\Gamma : \psi(\overline{\Gamma})\big)$ is finite, then using this we can prove that the subgroup 2Γ has a finite index in Γ.
Now, proving any one of statements, the index $\big(\overline{\Gamma} : \phi(\Gamma)\big)$ is finite or the index $\big(\Gamma : \psi(\overline{\Gamma})\big)$ is finite is enough. So we will just prove the second one. Thus we will prove following 5 propositions to prove this part:

Proposition 1: *Let $\mathbb{Q}^*$ be the multiplicative group of non-zero rational numbers, and $\mathbb{Q}^{*2}$ be the subgroup of squares of elements of $\mathbb{Q}^*$. Then a map $\alpha : \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$, defined by: $\alpha(\mathcal{O}) = 1 \bmod \mathbb{Q}^{*2}$, $\alpha(T) = b \bmod \mathbb{Q}^{*2}$ and $\alpha(x, y) = x \bmod \mathbb{Q}^{*2}$ if $x \neq 0$; is a homomorphism.*
Observe that, α sends inverses to inverses, because: $x \equiv \frac{1}{x} \pmod{\mathbb{Q}^{*2}}$

$$\alpha(-P) = \alpha(x, -y) = x \bmod \mathbb{Q}^{*2} \qquad \text{and} \qquad \alpha(P)^{-1} = \alpha\left(\frac{1}{x}, \frac{1}{y}\right) = \frac{1}{x} \bmod \mathbb{Q}^{*2}$$

Thus to prove this proposition, it is enough to show that whenever $P_1 + P_2 + P_3 = \mathcal{O}$, then $\alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv 1 \pmod{\mathbb{Q}^{*2}}$.
The triples of points which add to zero consist of the intersections of the curve with the line. If the line is $y = \lambda x + \nu$ and the x coordinates of the points of intersection are roots of following equation [put $c = 0$ in Theorem 1.8.1]

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x - \nu^2 = 0$$

Thus, from the product of roots relation:

$$x_1x_2x_3 = \nu^2 \in \mathbb{Q}^{*2}$$

Therefore,

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = x_1x_2x_3 = \nu^2 \equiv 1 \pmod{\mathbb{Q}^{*2}}$$

This proves the case that P_1, P_2, P_3 are distinct from $\mathcal{O}$ and T.
For other cases, proceed similar to Theorem 1.8.5(i).

Proposition 2: *The kernel of α is the image $\psi(\overline{\Gamma})$. Hence α induces a one-to-one homomorphism: $\frac{\Gamma}{\psi(\overline{\Gamma})} \hookrightarrow \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$*
From Theorem 1.8.5(iii), $\psi(\overline{\Gamma})$ is the set of points $(x, y) \in \Gamma$ such that x is a non-zero rational square, together with $\mathcal{O}$ and also T if b is a perfect square. Now comparing the definition of α with this description of $\psi(\overline{\Gamma})$, it is clear that the kernel of α is precisely $\psi(\overline{\Gamma})$.

Proposition 3: *Let $p_1, p_2, \ldots p_t$ be the distinct primes dividing b. Then the image of α is contained in the subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ consisting of the elements: $\{\pm p_1^{\sigma_1} p_2^{\sigma_2} \ldots p_t^{\sigma_t}$: each σ_i equals 0 or 1$\}$.*
As seen in Part-2, we know that rational points have coordinates of the form $x = m/e^2$ and $y = n/e^2$. Substituting this into given equation of curve we get:

$$n^2 = m^3 + am^2e^2 + bme^4 = m(m^2 + ame^2 + be^4)$$

This equation expresses the square n^2 as a product of two integers. In general case let

$$d = \gcd(m, m^2 + ame^2 + be^4)$$

Then d divides both m and be^4. But, m and e are relatively prime, since we assumed that x was written in lowest terms. Therefore, $d \big| b$.
Since, also $n^2 = m(m^2 + ame^2 + be^4)$ we deduce that every prime dividing m appears to an even power except possibly for primes dividing b. Therefore:

$$m = \pm W^2 \cdot p_1^{\sigma_1} p_2^{\sigma_2} \ldots p_t^{\sigma_t}$$

where W is some integer, each σ_i equals 0 or 1 and $p_1, p_2, \ldots p_t$ are distinct primes dividing b.
Thus:

$$\alpha(P) = x = \frac{m}{e^2} \equiv \pm p_1^{\sigma_1} p_2^{\sigma_2} \ldots p_t^{\sigma_t} \pmod{\mathbb{Q}^{*2}}$$

Thus proves the proposition for $x \neq 0$. But if $x = 0$, and hence $m = 0$, then by definition, $\alpha(T) = b \bmod \mathbb{Q}^{*2}$, shows the conclusion is still valid because $b = \cdot p_1^{\sigma_1} p_2^{\sigma_2} \ldots p_t^{\sigma_t}$ as indicated above.

Proposition 4: *The index* $(\Gamma : \psi(\overline{\Gamma}))$ *is at most* 2^{t+1}.

The subgroup described in previous proposition has precisely 2^{t+1} elements. On the other hand proposition 2 says that quotient group $\Gamma/\psi(\overline{\Gamma})$ maps one-to-one into this subgroup. Hence index of $\psi(\overline{\Gamma})$ inside Γ is at most 2^{t+1}.

Proposition 5: *Since,* $\psi(\overline{\Gamma})$ *has a finite index in* Γ, *we can find elements* $P_1, P_2, \ldots, P_n$ *representing the finitely many cosets. Similarly, since* $\phi(\Gamma)$ *has a finite index in* $\overline{\Gamma}$, *we can choose elements* $\overline{P}_1, \overline{P}_2, \ldots, \overline{P}_m$ *representing the finitely many cosets. Then the set,* $\{P_i + \psi(\overline{P}_j) : 1 \leq i \leq n, 1 \leq j \leq m\}$ *includes complete set of representatives for the cosets of* 2Γ *inside* Γ.

We know that Γ and $\overline{\Gamma}$ are abelian groups and in Theorem 1.8.5, we proved that for two homomorphisms $\phi : \Gamma \to \overline{\Gamma}$ and $\psi : \overline{\Gamma} \to \Gamma$:

$$\begin{cases} (\psi \circ \phi)(P) = 2P & \text{for all } P \in \Gamma \\ (\phi \circ \psi)(\overline{P}) = 2\overline{P} & \text{for all } \overline{P} \in \overline{\Gamma} \end{cases}$$

Further in previous proposition we proved that, $\psi(\overline{\Gamma})$ has a finite index in Γ, which as stated earlier, also proves that, $\phi(\Gamma)$ has a finite index in $\overline{\Gamma}$.

Let, $P \in \Gamma$. We need to show that P can be written as the sum of an element of this set plus an element of 2Γ.

Since, $P_1, P_2, \ldots, P_n$ are representatives for the cosets of $\psi(\overline{\Gamma})$ inside Γ, we can find some P_i so that $P - P_i \in \psi(\overline{\Gamma})$, say $P - P_i = \psi(\overline{P})$.

Also, $\overline{P}_1, \overline{P}_2, \ldots, \overline{P}_n$ are representatives for the cosets of $\phi(\Gamma)$ inside $\overline{\Gamma}$, we can find some $\overline{P}_i$ so that $\overline{P} - \overline{P}_i \in \psi(\Gamma)$, say $\overline{P} - \overline{P}_j = \phi(P')$.

Then,

$$P = P_i + \psi(\overline{P}) = P_i + \psi(\overline{P}_j + \phi(P'))$$

Now using Theorem 1.8.5

$$P = P_i + \psi(\overline{P}_j) + (\psi \circ \phi)(P') = P_i + \psi(\overline{P}_j) + 2P'$$

This completes proof of this part.

Part 5: *The above four parts imply that* Γ *is finitely generated.*

We know that there are only finitely many cosets of 2Γ in Γ, say n of them. Let $Q_1, Q_2, \ldots, Q_n$ be representatives for these cosets. Thus for any element $P \in \Gamma$, there is an index i_1, depending on P, such that, $P - Q_{i_1} \in 2\Gamma$. But, P has to be in one of the cosets, thus we can write $P - Q_{i_1} = 2P_1$. Continuing this process, we can write:

$$P_1 - Q_{i_2} = 2P_2$$
$$P_2 - Q_{i_3} = 2P_3$$
$$\vdots$$
$$P_{m-1} - Q_{i_m} = 2P_m$$

where $Q_{i_1}, Q_{i_2}, \ldots, Q_{i_m}$ are chosen from the coset representatives $Q_1, Q_2, \ldots, Q_n$ and $P_1, P_2, \ldots, P_m$ are elements of Γ.

Since we have, $P = Q_{i_1} + 2P_1$, now substitute the second equation, $P = Q_{i_1} + 2Q_{i_2} + 4P_2$, continuing in this way we get:

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \ldots + 2^{m-1}Q_{i_m} + 2^m P_m$$

This, implies that P is in the subgroup of Γ generated by Q_i's and P_m.

In Part-2, replace P_0 with $-Q_i$, to get a constant, ε_i such that:

$$h(P - Q_i) \leq 2h(P) + \varepsilon_i \qquad \text{for all } P \in \Gamma$$

Now, do this for each Q_i, $1 \leq i \leq n$. Let ε' be the largest of all ε_i's. Then:

$$h(P - Q_i) \leq 2h(P) + \varepsilon' \qquad \text{for all } P \in \Gamma \quad \text{and all } 1 \leq i \leq n$$

We can do this because there are only finitely many Q_i's, from Part-4.
Let, ε be the constant from Part-3. Then we can calculate:

$$4h(P_j) \leq h(2P_j) + \varepsilon = h(P_{j-1} - Q_{i_j}) + \varepsilon \leq 2h(P_{j-1}) + \varepsilon' + \varepsilon$$

$$\Rightarrow h(P_j) \leq \frac{1}{2}h(P_{j-1}) + \frac{\varepsilon + \varepsilon'}{4} = \frac{3}{4}h(P_{j-1}) - \frac{1}{4}\left(h(P_{j-1}) - (\varepsilon + \varepsilon')\right)$$

Now, if $h(P_{j-1}) \geq \varepsilon + \varepsilon'$

$$\Rightarrow h(P_j) \leq \frac{3}{4}h(P_{j-1})$$

So, in the sequence of points $P, P_1, P_2, P_3, \ldots$, as long as the point P_j satisfies the condition $h(P_j) \geq \varepsilon + \varepsilon'$, then the next point in the sequence has much smaller height, namely, $h(P_{j+1}) \leq \frac{3}{4}h(P_j)$.
But, if we start with a number and keep multiplying it by 3/4, then it approaches zero. So eventually we will find an index m such that, $h(P_m) \leq \varepsilon + \varepsilon'$.
Thus we have shown that every element $P \in \Gamma$ can be written in the form:

$$P = a_1Q_1 + a_2Q_2 + \ldots + a_nQ_n + 2^mR$$

for certain integers $a_1, a_2, \ldots, a_n$ and some point $R \in \Gamma$ satisfying the inequality $h(R) \leq \varepsilon + \varepsilon'$.
Hence the set:

$$\{Q_1, Q_2, \ldots, Q_n\} \cup \{R \in \Gamma : h(R) \leq \varepsilon' + \varepsilon\}$$

generates Γ.
From Part-1 and Part-4, this set is finite, which completes the proof that Γ is finitely generated.

□

Remark: There is no known method to determine in a finite number of steps whether a given rational cubic has rational point.

Example 1.8.1. *Solve*

$$y^2 = x^3 - x$$

in rational numbers.

Solution. Let us denote given curve by C, so

$$C : y^2 = x^3 - x$$

Now we will borrow all notations from proof of Theorem 1.8.6, and we get: $a = 0, b = -1$.
Next task is to determine the rank of $C(\mathbb{Q}) = \Gamma$ denoted by r. The group Γ will be finite if and only if it has rank, r, equal to zero[30]. Thus we will use following formula to calculate rank of Γ:

$$2^r = \frac{\#\alpha(\Gamma) \cdot \#\overline{\alpha}(\overline{\Gamma})}{4} \tag{1.20}$$

Where, $(\Gamma : \psi(\overline{\Gamma})) = \#\alpha(\Gamma)$ and $(\overline{\Gamma} : \psi(\Gamma)) = \#\overline{\alpha}(\overline{\Gamma})$. Also, $\overline{\alpha}$ is defined similar to α, as, $\overline{\alpha} : \overline{\Gamma} \to \mathbb{Q}^*/\mathbb{Q}^2$, such that by:

$$\begin{cases} \overline{\alpha}(\overline{\mathcal{O}}) = 1 \bmod \mathbb{Q}^2, \\ \overline{\alpha}(\overline{T}) = \overline{b} \bmod \mathbb{Q}^2, \\ \overline{\alpha}(\overline{x}, \overline{y}) = \overline{x} \bmod \mathbb{Q}^2 \quad \text{if } \overline{x} \neq 0 \end{cases}$$

To determine, $\#\alpha(\Gamma)$ (called *order of* $\alpha(\Gamma)$), we will write down several equations of form:

$$N^2 = b_1M^4 + aM^2e^2 + b_2e^4$$

one for each factorization $b = b_1b_2$.We will decide whether or not each of these equations has a solution in integers with $M \neq 0$ and each time we find an equation with a solution (M, e, N), then we get a new point on the curve by the formula:

$$x = \frac{b_1M^2}{e^2}, \qquad y = \frac{b_1MN}{e^3}$$

---

[30] For proof refer pp. 89-91 of [10]

Thus for each b_1, b_2, either exhibit a solution or show that the equation has no solution by using Modulo Arithmetic & Parity or as an equation in real numbers.

The first step is to factor b in all possible ways. There are two factorizations in this case:

$$-1 = -1 \times 1 \qquad \text{and} \qquad -1 = 1 \times -1$$

Thus b_1 can be only ± 1. Since $\alpha(\mathcal{O}) = 1$ and $\alpha(T) = b = -1$, we see that:

$$\alpha(\Gamma) = \{\pm 1 \bmod \mathbb{Q}^{*2}\}$$

is a group of two elements or $\#\alpha(\Gamma) = 2$.
Next we have to compute, $\overline{\alpha}(\overline{\Gamma})$, so we need to apply above procedure to:

$$\overline{C} : y^2 = x^3 + 4x$$

Now, $\overline{b} = 4$, has lots of factorizations; we can choose:

$$b_1 = 1, -1, 2, -2, 4, -4$$

But, $4 \equiv 1 \pmod{\mathbb{Q}^{*2}}$ and $-4 \equiv -1 \pmod{\mathbb{Q}^{*2}}$, so $\overline{\alpha}(\overline{\Gamma})$ consists of at most the four elements $\{1, -1, 2, -2\}$.
Clearly we have $\overline{b} \in \overline{\alpha}(\overline{\Gamma})$, but in this case, $\overline{b} = 4$ is a square, so this doesn't help us in this case.
Hence the four equations we must consider are:

$$(i) \quad N^2 = M^4 + 4e^4 \qquad\qquad (ii) \quad N^2 = -M^4 - 4e^4$$

$$(iii) \quad N^2 = 2M^4 + 2e^4 \qquad\qquad (iv) \quad N^2 = -2M^4 + -2e^4$$

Since, $N^2 \geq 0$, and we do not allow solutions with $M = 0$, we see that equations (i) and (iv) have no solutions in integers (in fact they have no solutions in real numbers with $M \neq 0$).
Equation (i) has trivial solution $(M, e, N) = (1, 0, 1)$, which corresponds to the fact that $1 \in \overline{\alpha}(\overline{\Gamma})$.
Also (1.20), tells us that $\#\alpha(\Gamma) \cdot \#\overline{\alpha}(\overline{\Gamma})$ is atleast 4, so in this example, we know that $\#\overline{\alpha}(\overline{\Gamma})$ is at least two.
Thus equation (iii) must have a solution. In fact we can see that:

$$2^2 = 2 \cdot 1^4 + 2 \cdot 1^4$$

So we conclude that $\#\overline{\alpha}(\overline{\Gamma}) = 2$.
Thus rank of Γ is zero, and the same is true for rank of $\overline{\Gamma}$, so we can solve both C and $\overline{C}$ using same arguments.
Thus the group of rational points on C and $\overline{C}$ are both finite, and so all rational points have finite order.
Now to find points of finite order, we can use Theorem 1.8.4 (Nagell-Lutz Theorem). Thus, if $P = (x, y)$ is a point of finite order in Γ, then either $y = 0$ or $y \big| b^2(a^2 - 4b) \Rightarrow y \big| 4$. The points with $y = 0$ are $(0, 0)$ and $(\pm 1, 0)$ and for $y = \pm 2, \pm 3, \pm 4$, we get no points. Thus the group of rational points on$C$ are:

$$C(\mathbb{Q}) = \{\mathcal{O}, (0,0), (1,0), (-1,0)\}$$

Similarly, we can find points of finite order in $\overline{\Gamma}$, as $y = 0$ or $y \big| \overline{b}^2(\overline{a}^2 - 4\overline{b}) \Rightarrow y \big| -256$. Proceeding in same way as for C, we get:

$$\overline{C}(\mathbb{Q}) = \{\mathcal{O}, (0,0), (2,4), (2,-4)\}$$

Example 1.8.2. *Solve*

$$y^2 = x^3 + 20x$$

in rational numbers.

Solution. Unlike previous example, here you will get rank of Γ to be 1. Thus it has infinitely many solutions. [To eliminate some equations you will have to use Fermat's Little Theorem]

Chapter 2

Special Types of Diophantine Equations

Here I will discuss few of the well studied types of diophantine equations. A complete list of well studied diophantine equations upto year 1969, can be found pp. 307 onwards in [5].

2.1 Linear Equations

2.1.1 Equations in two unknowns

Theorem 2.1.1. *Let* $a, b, c \in \mathbb{Z}$; $a, b \neq 0$. *Consider the linear diophantine equation* $ax + by = c$, *then:*

i. *If* $d = \gcd(a, b)$ *then this linear equation is solvable in integers if and only if* $d \mid c$.

ii. *If* (x_0, y_0) *is a particular solution of this equation then every integer solution is of the form:*

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t$$

where $t \in \mathbb{Z}$.

Sketch of Proof. The basic idea behind proof is:

i. Apply Euclid's Division Algorithm in bottom-up fashion

ii. Simply substitute given solution in diophantine equation and verify.

Methods to find particular solution. There are two methods available:

1. Remainder Substitution & Isolation
2. Last Partial Quotient Omission & Subtraction

Actually both methods are equivalent and are based on Euclid's Division Algorithm. The proof of equivalence between both methods requires *theory of Continued Fractions* which I will not discuss here. For proof you may refer [7] or [15].

I will illustrate both methods using following example:

Example 2.1.1. *Solve* $127x - 52y + 1 = 0$ *for integers.*

Solution. Firstly we will calculate $\gcd(127, 52)$

$$127 = 52 \times 2 + 23$$

$$52 = 23 \times 2 + 6$$

$$23 = 6 \times 3 + 5$$

$$6 = 5 \times 1 + 1$$

$$5 = 1 \times 5 + 0$$

Since $\gcd(127, 52) = 1$ this equation is solvable.

Method 1: The first step is to rewrite the equation first step of division algorithm as:

$$23 = a - 2b, \qquad \text{where we let } a = 127 \quad \& \quad b = 52$$

Next we substitute this value into second equation and also replace 52 by b:

$$b = (a - 2b) \times 2 + 6$$

Now rearrange the terms and isolate the reminder:

$$6 = 5b - 2a$$

Now substitute 6 and 23 in terms of a and b in next equation of division algorithm:

$$a - 2b = (5b - 2a) \times 3 + 5$$

Again rearrange terms and isolate remainder:

$$5 = 7a - 17b$$

Now substitute 5 and 6 in next equation of division algorithm:

$$5b - 2a = (7a - 17b) \times 1 + 1$$

Now rearrange the terms to get:

$$9a - 22b + 1 = 0$$

Comparing with given equation we get: $x = 9$ and $y = 22$ as a particular solution. From this we can generate all infinite solutions.

Method 2: First step is to create an improper fraction by dividing bigger coefficient by smaller coefficient (magnitude only)
Thus in this example we get: $\frac{127}{52}$
Now separate out the integral part of this fraction:

$$\frac{127}{52} = 2 + \frac{23}{52}$$

Then re-write the fractional part in terms of terminating continued fraction as:

$$\frac{127}{52} = 2 + \frac{23}{52} = 2 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{5}}}}$$

Now we will omit the last partial quotient and simplify the continued fraction so formed:

$$2 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1}}} = \frac{22}{9}$$

Now we will subtract this new fraction from our original improper fraction:

$$\frac{127}{52} - \frac{22}{9} = \frac{-1}{52 \times 9}$$

Cross multiply denominators to get:

$$127 \times 9 - 52 \times 22 + 1 = 0$$

Compare it with original equation and get $x = 9$ and $y = 22$ as a particular solution.

Remark: Note that both the methods described above lead to same solutions, which provides a verification to my assertion that at base level both methods are equivalent. It may be noted that these methods provide the least solution of the equation, namely that for which $x < |b|$ and $y < |a|$.

2.1.2 Equations in $n-$unknowns

Theorem 2.1.2. *Given a linear equation:*

$$a_1x_1 + a_2x_2 \dots + a_nx_n = c$$

where $n \geq 2$, $a_1, a_2, \dots, a_n, c$ *are fixed integers and all coefficients* $a_1, a_2, \dots, a_n$ *are different from zero.*

i. This equation is solvable if and only if $\gcd(a_1, a_2, \dots, a_n)|c$.

ii. If this equation is solvable then one can choose $n-1$ *solutions such that each solution is an integer linear combination of those* $n-1$ *solutions.*

Sketch of Proof. These generalizations can be proved by induction on basic case of $n = 2$.(Theorem 2.1.1)

i. Let $d = \gcd(a_1, \dots, a_n)$. If c is not divisible by d, then given equation is not solvable.

ii. Actually, we need to prove that $\gcd(x_1, x_2, \dots, x_n)$ is a linear combination with integer coefficients of $x_1, x_2, \dots, x_n$. Apply induction on Euclid's Division Algorithm which we use to create linear combination for two numbers. Since: $\gcd(x_1, \dots, x_n) = \gcd(\gcd(x_1, \dots, x_{n-1}), x_n)$.

Theorem 2.1.3. *Suppose that the equation:*

$$a_1x_1 + a_2x_2 + \dots + a_mx_m = n$$

where $a_1, a_2, \dots, a_m > 0$*, is solvable in non-negative integers, and let* A_n *be the number of its solutions* $(x_1, x_2, \dots, x_m)$*. Then:*

$$A_n = \frac{1}{n!}f^n(0)$$

where,

$$f(x) = \frac{1}{(1-x^{a_1})(1-x^{a_2})\dots(1-x^{a_m})}, \quad |x| < 1$$

is the generating function of the sequence $\{A_n\}_{n\geq 1}$*. and* $f^n(x_0)$ *denotes the* n^{th} *derivative of* $f(x)$ *at point* x_0*.*

Remark: A generating function $f(x)$ is a power series function of variable x, that is, we can substitute in a value of x and if the power series is converging series then we get back value of $f(x)$. Generating function for a given sequence has the terms of the sequence as coefficients of the power series. For examples refer Chapter 41 of [16]

Proof. Note that if $n = 0$ and if all coefficients are positive then only one trivial non-negative solution namely $(0, 0, \dots, 0)$ exist, thus $A_0 = 1$. Hence we can write our sequence as:

$$A_0, A_1, A_2, A_3, A_4 \dots$$

thus the corresponding generating function $f(x)$ will be:

$$f(x) = A_0 + A_1x + A_2x^2 + A_3x^3 + A_4x^4 + \dots \tag{2.1}$$

Now let's observe the most important generating function i.e *Geometric Series Formula* (Note that this is generating function for sequence $1, 1, 1, 1, 1, 1, \dots$):

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots, \quad |x| < 1$$

We have a_i as our coefficients so we consider geometric series of form:

$$\frac{1}{1-x^{a_i}} = 1 + x^{a_i} + x^{2a_i} + x^{3a_i} + \dots, \quad |x| < 1$$

A_n is the number of non-negative solutions of given linear diophantine equation which is exactly same as the number of ways we can add the exponents of x i.e. αa_i, where $\alpha \in \mathbb{Z}^+$ to get n in exponent (since linear diophantine equation is essentially linear combination of coefficients) thus we can write $f(x)$ as:

$$f(x) = (1 + x^{a_1} + x^{2a_1} + \dots)(1 + x^{a_2} + x^{2a_2} + \dots)\dots(1 + x^{a_m} + x^{2a_m} + \dots), \quad |x| < 1 \tag{2.2}$$

Replace RHS by geometric series formula to get the desired generating function:

$$f(x) = \frac{1}{(1-x^{a_1})(1-x^{a_2})\dots(1-x^{a_m})}, \quad |x| < 1$$

Thus by comparing (2.1) and (2.2) we can say that A_n is the coefficient of x^n we get on multiplication of all brackets. We can find that coefficient easily using basic calculus on (2.1). Observe that:

$$f^n(x) = n!A_n + \frac{(n+1)!}{1!}(n+1)!A_{n+1}x + \frac{(n+2)!}{2!}A_{n+2}x^2 + \frac{(n+3)!}{3!}A_{n+3}x^3 + \dots \tag{2.3}$$

Thus we can separate out A_n as:

$$A_n = \frac{1}{n!}f^n(0)$$

□

Remark: Though this formula for finding number of non-negative solutions of a given linear diophantine equation with positive coefficients is easy to derive but calculation of A_n using this formula is difficult in most situations(see [14]). Note that computing the number solutions of even a linear diophantine equation is by far one the most complex process.

2.2 Equations of second degree in two unknowns

2.2.1 Equations of form: $x^2 - Dy^2 = 1$, $D \in \mathbb{Z}^+$ and $\sqrt{D}$ is irrational

Diophantus considered only rational solutions of such equations, but other mathematicians like Brahmagupta, Jayadeva, Bhaskaracharya, Fermat, Euler, and others focused on its solutions in integers. Note that this equation has the trivial solution $(x_0, y_0) = (1, 0)$ in non-negative integers. I will here study such equations using elementary arithmetic. But, we can also handle such equations using concept of *Unique Factorization Domains*, for that treatment refer pp. 167-169 of [17].

Theorem 2.2.1. *Given an equation:*

$$x^2 - Dy^2 = 1$$

where $D \in \mathbb{Z}^+$ *and* $\sqrt{D}$ *is irrational*[1]

i. *This equation possesses a non-trivial solution* (x_1, y_1) *in positive integers.*

ii. *The general solution is given by* (x_n, y_n), $n \geq 0$,

$$\begin{cases} x_{n+1} = x_1 x_n + D y_1 y_n \\ y_{n+1} = y_1 x_n + x_1 y_n, \end{cases}$$

where (x_1, y_1) *is the least solution. Hence this equation has infinitely many solutions in non-negative integers.*

iii. *Show that:*

$$\begin{cases} x_n = 2x_1 x_{n-1} - x_{n-2} \\ y_n = 2x_1 y_{n-1} - y_{n-2} \end{cases} \quad \textit{for} \quad n \geq 2$$

also gives general solution of this equation.

iv. *If* (x_1, y_1) *is the least solution of the equation then any solution of the equation is of form* $(\pm x_n, \pm y_n)$, *where*

$$\begin{cases} x_n = \frac{1}{2}[(x_1 + y_1\sqrt{D})^n + (x_1 - y_1\sqrt{D})^n] \\ y_n = \frac{1}{2\sqrt{D}}[(x_1 + y_1\sqrt{D})^n - (x_1 - y_1\sqrt{D})^n] \end{cases}$$

---

[1] The equation is of no interest when D is a perfect square, since the difference of two perfect squares can never be 1, except in the case $1^2 - 0^2$

Remark: (x_1, y_1) is called the least solution or minimal solution of equation if for $x = x_1$ and $y = y_1$ the binomial $x + y\sqrt{D}$, assumes the least possible value among all the possible values which it will take when all the possible positive integral solutions of the equation are substituted for x and y.

Proof. Before we start the proof you must have an understanding of terms like *Sequences*, *Convergent of a continued fractions*[2] (for details see [15]) and *Greatest Integer Function* (denoted by $\lfloor\bullet\rfloor$).

i. We will divide the proof into three parts[3]

   a. Prove the existence of a positive integer k such that equation $x^2 - Dy^2 = k$ has an infinite number of positive integral solutions.

   Given:

$$x^2 - Dy^2 = (x - \sqrt{D}y)(x + \sqrt{D}y) = k \tag{2.4}$$

   Now consider an even convergent of the irrational number $\sqrt{D}$, $\delta_{2n} = \frac{P_{2n}}{Q_{2n}} > \sqrt{D}$. Replace x and y respectively by the numerator and denominator of this even convergent to get:

$$P_{2n}^2 - DQ_{2n}^2 = (P_{2n} - \sqrt{D}Q_{2n})(P_{2n} + \sqrt{D}Q_{2n})$$

   The left hand side of this equality, and therefore the right hand side too, is an integer. Let it be z_{2n} and $\sqrt{D} = \alpha$ Then we can write:

$$z_{2n} = (P_{2n} - \alpha Q_{2n})(P_{2n} + \alpha Q_{2n}) \tag{2.5}$$

   But since:

$$\begin{cases} 0 < P_{2n} - \alpha Q_{2n} < \frac{1}{Q_{2n+1}} \\ 0 < P_{2n} + \alpha Q_{2n} = 2\alpha Q_{2n} + P_{2n} - \alpha Q_{2n} < 2\alpha Q_{2n} + \frac{1}{Q_{2n+1}} \end{cases}$$

   Now substitute these inequalities in (2.5) to estimate z_{2n}.

$$0 < z_{2n} < \frac{1}{Q_{2n+1}}\left(2\alpha Q_{2n} + \frac{1}{Q_{2n+1}}\right) < 2\alpha + 1$$

   since $Q_{2n} < Q_{2n+1}$.
   But z_{2n} is an integral positive value. Thus, all numbers $z_2, z_4, \ldots, z_{2n}, \ldots$ will be positive integers, none of which exceed the same number $2\alpha + 1$. But since $\alpha = \sqrt{D}$ is irrational, its continued fraction is infinite and so the sequence of pairs of numbers P_{2n} and Q_{2n} is also infinite.
   Now since there are not more than $\lfloor 2\alpha + 1\rfloor$ integers between 1 and the number $2\alpha + 1$ (which is definite and does not depend on n), the infinite sequence of positive integers $z_2, z_4, \ldots, z_{2n}, \ldots$ is made up of a finite number of different terms.
   In other words, the infinite number series $z_2, z_4, \ldots, z_{2n}, \ldots$ is just the sequence of integers $1, 2, 3, \ldots, \lfloor 2\alpha + 1\rfloor$ repeated in some way or other and it is not even necessary for all these integers to occur in the series.
   Note also that since the quantity of different terms of the infinite series $z_2, z_4, \ldots, z_{2n}, \ldots$ is finite, at least one term (one number), k $(1 \le k \le \lfloor 2\alpha + 1\rfloor)$, is repeated an infinite number of times.
   Hence, among the pairs of numbers $(P_2, Q_2), (P_4, Q_4), \ldots, (P_{2m}, Q_{2n}), \ldots$ there is an infinite set of pairs for which $z = x^2 - Dy^2$ assumes the same value k upon substitution of these numbers in

---

[2] The expression obtained by omitting all terms of its continued fraction (of say α) starting with some particular term is called *convergent*. The first convergent δ_1 is equal to first partial quotient (q_0). Also convergents satisfy following inequality: $\delta_1 < \delta_3 < \ldots < \delta_{2k-1} < \alpha$ and $\delta_2 > \delta_4 > \ldots > \delta_{2k} > \alpha$. Also we can write k^{th} convergent as: $\delta_k = \frac{P_k}{Q_k}$, $(1 \le k \le n)$ Then we write a recursive formula:

$$\begin{cases} P_k = P_{k-1}q_k + P_{k-2} \\ Q_k = Q_{k-1}q_k + Q_{k-2} \end{cases}$$

Also for consecutive convergents:

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_kQ_{k-1}} \quad (k > 1)$$

[3] There is an elegant way of proving this assertion using *Diophantine Approximation* which is based on *Pigeon Hole Principle*, for that proof refer pp. 232 of [16] or pp. 53 of [5].

place of x and y.
Thus, we have proved the existence of a positive integer k for which (2.4) possesses an infinite number of integral solutions (x, y).

b. Prove that among the pairs of integers which are solution of (2.4) for given k, there will be infinitely many pairs yielding the same remainders when divided by k

If we could assert that $k = 1$, then we would have proved that given equation has an infinite number of integral solutions. Since we cannot assert this, let us assume that $k > 1$ (in the contrary case when $k = 1$ everything is proved).
We can put the statement to be proved in another way, we shall prove that there exist two non-negative integers, p and q, both less than k, such that for an infinite number of pairs $(u_1, v_1), (u_2, v_2), \ldots, (u_n, v_n), \ldots$ which are solutions of:

$$u_n^2 - Dv_n^2 = k \tag{2.6}$$

the equalities:

$$\begin{cases} u_n = a_n k + p \\ v_n = b_n k + q \end{cases} \tag{2.7}$$

hold, where a_n and b_n are the quotients upon division of u_n and v_n by k, and p and q the remainders.
For, if we divide u_n and v_n by the integer k, $k > 1$, then we obtain relations of this form, where as always the remainders upon division lie between zero and $k - 1$.
Since the only possible remainders upon the division of the numbers u_n by k are the numbers $0, 1, 2, \ldots, k-1$, and likewise the remainders upon the division of v_n by k can only be these same numbers $0, 1, 2, \ldots, k-1$, then the number of possible pairs of remainders upon the division of the numbers u_n, and v_n by k will be $k \times k = k^2$.
This is also obvious because a pair of remainders (p_n, q_n) corresponds to each pair (u_n, v_n) and the number of different values assumed by each of the numbers p_n and q_n separately is not greater than k.
Consequently, the number of different pairs of remainders is not greater than k^2.
Thus to each pair of integers (u_n, v_n) there corresponds a pair of remainders (p_n, q_n) on division by k.
But the number of different pairs of remainders is finite, does not exceed k^2 , while the number of pairs (u_n, v_n) is infinite.
This means that since the number of different pairs in the sequence $(p_1, q_1), (p_2, q_2), \ldots, (p_n, q_n), \ldots$ is finite, at least one pair of remainders is repeated an infinite number of times.
Denoting this pair of remainders (p, q), we see that there exists an infinite set of pairs (u_n, v_n) for which relations (2.7) hold.
Since not all the pairs satisfy (2.7) for certain definite p and q, whose existence we have just proved, we shall renumber all those pairs $u_n, v_n)$ which satisfy (2.7) denoting them by (R_n, S_n).
So, the infinite sequence of pairs $(R_1, S_1), (R_2, S_2), \ldots, (R_n, S_n), \ldots$ is a subsequence of the sequence (u_n, v_n) which, in turn, is a subsequence of the sequence of numerators and denominators of the even convergents of α.
The pairs of numbers $(R_1, S_1), (R_2, S_2), \ldots, (R_n, S_n), \ldots$ satisfy equation (2.6) and yield the same remainders, p and q, on division by k.
Thus we have established the existence of an infinite set of such pairs of positive integers yielding the same remainders when divided by k.

c. Generate a general solution of $x^2 - Dy^2 = 1$

In last step we have established the existence of an infinite set of such pairs of positive integers R_n and S_n. Note first of all that the pairs (R_n, S_n), being the numerators and denominators of convergents, must be pairs of relatively prime numbers.

Indeed, if we replace k by $2k$ in

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_k Q_{k-1}} \quad (k > 1)$$

and set $\delta_{2k} = \frac{P_{2k}}{Q_{2k}}, \delta_{2k-1} = \frac{P_{2k-1}}{Q_{2k-1}}$, then we get:

$$\frac{P_{2k}}{Q_{2k}} - \frac{P_{2k-1}}{Q_{2k-1}} = \frac{1}{Q_{2k}Q_{2k-1}}$$

multiply both sides by $Q_{2k}Q_{2k-1}$, we get

$$P_{2k}Q_{2k-1} - P_{2k-1}Q_{2k} = 1$$

This relation between four integers, P_{2k}, Q_{2k}, P_{2k-1} and Q_{2k-1} shows that if P_{2k} and Q_{2k} have a common divisor greater than unity, then its whole left-hand side must be divisible by this common divisor. But the right-hand side of above equality is unity, which cannot be divided by any integer greater than unity.
Thus it is established that the numbers R_n and S_n, which can only be the numerators and denominators of convergents, are relatively prime.
From following relation:

$$\begin{cases} P_k = P_{k-1}q_k + P_{k-2} \\ Q_k = Q_{k-1}q_k + Q_{k-2} \end{cases}$$

it also immediately follows that: $Q_2 < Q_4 < \ldots < Q_{2n} < \ldots$
From the fact that the numbers R_n and S_n are relatively prime and $S_1, S_2, \ldots, S_n, \ldots$, which are taken from the sequence of numbers Q_{2n} all differing from one another, are also all different from one another, it immediately follows that in the infinite sequence of fractions:

$$\frac{R_1}{S_1}, \frac{R_2}{S_2}, \ldots, \frac{R_n}{S_n}, \ldots$$

there are no numbers equal to one another.
Note that the definition of numbers R_n and S_n is:

$$R_n^2 - DS_n^2 = (R_n - \alpha S_n)(R_n + \alpha S_n) = k, \quad (\alpha = \sqrt{D})$$

Now substitute (R_1, S_1) and (R_2, S_2) in this definition:

$$\begin{cases} R_1^2 - DS_1^2 = (R_1 - \alpha S_1)(R_1 + \alpha S_1) = k \\ R_2^2 - DS_2^2 = (R_2 - \alpha S_2)(R_2 + \alpha S_2) = k \end{cases} \tag{2.8}$$

Also,

$$(R_1 - \alpha S_1)(R_2 + \alpha S_2) = R_1R_2 - DS_1S_2 + \alpha(R_1S_2 - S_1R_2) \tag{2.9}$$

Similarly,

$$(R_1 + \alpha S_1)(R_2 - \alpha S_2) = R_1R_2 - DS_1S_2 - \alpha(R_1S_2 - S_1R_2) \tag{2.10}$$

When divided by k, R_n and S_n leave remainders p and q independent of n (as proved in earlier). Consequently, because of (2.7), we get:

$$\begin{cases} R_n = c_nk + p \\ S_n = d_nk + q \end{cases} \tag{2.11}$$

Now after a series of *High School Algebra*[4] transformations and substitutions using (2.8) and (2.11) we get:

$$R_1R_2 - DS_1S_2 = R_1(c_2k + p) - DS_1(d_2k + q) = k[R_1(c_2 - c_1) - DS_1(d_2 - d_1) + 1] = kx_1 \tag{2.12}$$

---

[4] As called by S. Abhyankar

where x_1 is a integer.
Similarly by using (2.11) only we get:

$$R_1S_2 - S_1R_2 = R_1(d_2k+q) - S_1(c_2k+p) = k[R_1(d_2-d_1) - S_1(c_2-c_1)] = ky_1 \tag{2.13}$$

where y_1 is again an integer.
We can assert that y_1 is not equal to zero i.e. this is non-trivial solution. For suppose $y_1 = 0$, then $ky_1 = R_1S_2 - R_2S_1 = 0$, hence, $\frac{R_1}{S_1} = \frac{R_2}{S_2}$ which is impossible since we have already proved that all these fractions $\frac{R_n}{S_n}$ are different.
Now use (2.12) and (2.13) in (2.9) and (2.10) to get:

$$\begin{cases}(R_1 - \alpha S_1)(R_2 + \alpha S_2) = k(x_1 + \alpha y_1)\\ (R_1 + \alpha S_1)(R_2 - \alpha S_2) = k(x_1 - \alpha y_1)\end{cases} \tag{2.14}$$

Use (2.14) in (2.8) to get:

$$k^2 = (R_1^2 - DS_1^2)(R_2^2 - DS_2^2) = k^2(x_1^2 - Dy_1^2)$$

Since $k > 0$ (we have already proved in first part), cancelling k^2, we get:

$$x_1^2 - Dy_1^2 = 1$$

But $y_1 \neq 0$ (we have already proved in this part) which means that $x_1 \neq 0$, otherwise the left-hand side would be negative while the right-hand side would be equal to unity. Thus, even under the assumption that $k \neq 1$ or $k > 1$, we have determined two non-zero integers, x_1 and y_1 which satisfy equation $x^2 - Dy^2 = 1$.

ii. Use induction with respect to n. Clearly, (x_1, y_1) is a solution to given equation. If (x_n, y_n) is a solution to this equation, then:

$$x_{n+1}^2 - Dy_{n+1}^2 = (x_1x_n + Dy_1y_n)^2 - D(y_1x_n + x_1y_n)^2 = (x_1^2 - Dy_1^2)(x_n^2 - Dv_n^2) = 1$$

thus the pair (x_{n+1}, y_{n+1}) is also a solution to the given equation.
Observe that for all non-negative integers (*this statement has simple proof by contradiction, refer, pp. 354-355 of [9]*)

$$(x_1 + y_1\sqrt{D})^n = x_n + y_n\sqrt{D} \tag{2.15}$$

Let, $z_n = x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n, n \geq 0$ and note that, $z_0 < z_1 < z_2 < \dots$
We will now prove that the solutions to given equation satisfy (2.15).
Indeed, if given equation has a solution (x, y) such that $z = x + y\sqrt{D}$ is not of the form (2.15), then $z_m < z < z_{m+1}$ for some integer m.
Then,

$$1 < \frac{z}{z_m} = \frac{(x + y\sqrt{D})}{(x_1 + y_1\sqrt{D})^m} = \frac{(x + y\sqrt{D})}{(x_m + y_m\sqrt{D})} = (x + y\sqrt{D})(x_m - y_m\sqrt{D}) < x_1 + y_1\sqrt{D}$$

and therefore,

$$1 < (xx_m + yy_m\sqrt{D}) + (x_my - xy_m\sqrt{D}) < x_1 + y_1\sqrt{D}$$

Whereas,

$$(xx_m - Dyy_m)^2 - D(x_my - xy_m)^2 = (x^2 - Dy^2)(x_m^2 - Dy_m^2) = 1$$

Thus, $(xx_m - Dyy_m, x_my - xy_m)$ is a solution of given equation, which is less than (x_1, y_1), contradicting the assumption that (x_1, y_1) was minimal or least solution

iii. The the relation:

$$\begin{cases}x_{n+1} = x_1x_n + Dy_1y_n\\ y_{n+1} = y_1x_n + x_1y_n,\end{cases}$$

can be written in matrix[5] form as:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix}$$

Which leads to:

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{bmatrix} \begin{bmatrix} x_{n-1} \\ y_{n-1} \end{bmatrix} = \begin{bmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{bmatrix}^2 \begin{bmatrix} x_{n-2} \\ y_{n-2} \end{bmatrix} = \ldots = \begin{bmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{bmatrix}^n \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} \tag{2.16}$$

where $(x_0, y_0) = (1, 0)$ is the trivial solution
Let's calculate:

$$\begin{bmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{bmatrix}^2 = \begin{bmatrix} x_1^2 + Dy_1^2 & 2Dy_1x_1 \\ 2x_1y_1 & Dy_1^2 + x_1^2 \end{bmatrix}$$

From previous part, we know $x_2 = x_1^2 + Dy_1^2$, $y_2 = 2y_1x_1$:

$$\begin{bmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{bmatrix}^2 = \begin{bmatrix} x_2 & Dy_2 \\ y_2 & x_2 \end{bmatrix} \tag{2.17}$$

Since $x_1^2 - Dy_1^2 = 1$ we get:

$$\begin{bmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{bmatrix}^2 = \begin{bmatrix} 2x_1^2 - 1 & 2Dx_1y_1 \\ 2x_1y_1 & 2x_1^2 - 1 \end{bmatrix}$$

Thus:

$$\begin{bmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{bmatrix}^2 = 2x_1 \begin{bmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Further since, where $(x_0, y_0) = (1, 0)$ is the trivial solution, we get:

$$\begin{bmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{bmatrix}^2 = 2x_1 \begin{bmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{bmatrix} - \begin{bmatrix} x_0 & y_0 \\ y_0 & x_0 \end{bmatrix} \tag{2.18}$$

Equating (2.17) and (2.18) we get:

$$\begin{bmatrix} x_2 & Dy_2 \\ y_2 & x_2 \end{bmatrix} = 2x_1 \begin{bmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{bmatrix} - \begin{bmatrix} x_0 & y_0 \\ y_0 & x_0 \end{bmatrix}$$

Now by induction on (2.17) and (2.18), we get:

$$\begin{bmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{bmatrix}^n = \begin{bmatrix} x_n & Dy_n \\ y_n & x_n \end{bmatrix} = 2x_1 \begin{bmatrix} x_{n-1} & Dy_{n-1} \\ y_{n-1} & x_{n-1} \end{bmatrix} - \begin{bmatrix} x_{n-2} & y_{n-2} \\ y_{n-2} & x_{n-2} \end{bmatrix} \tag{2.19}$$

Using (2.19) in (2.16) after substituting $x_0 = 1$ and $y_0 = 0$ we get:

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = 2x_1 \begin{bmatrix} x_{n-1} \\ y_{n-1} \end{bmatrix} - \begin{bmatrix} x_{n-2} \\ y_{n-2} \end{bmatrix} \tag{2.20}$$

Thus,

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 2x_1x_{n-1} - x_{n-2} \\ 2x_1y_{n-1} - y_{n-2} \end{bmatrix}$$

Hence we have obtained the required formula for x_n and y_n:

$$\begin{cases} x_n = 2x_1x_{n-1} - x_{n-2} \\ y_n = 2x_1y_{n-1} - y_{n-2} \end{cases} \quad \text{for} \quad n \geq 2$$

---

[5] Note that:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} p \\ q \end{bmatrix} = \begin{bmatrix} ap + bq \\ cp + dq \end{bmatrix} \qquad \& \qquad \begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} pa + qc & pb + qd \\ ra + sc & rb + sd \end{bmatrix}$$

iv. Now we will have to find corresponding generating function, for recursive formula proved in previous part so as to explicitly find n^{th} term.
Since x_n and y_n both are of same form, for the ease of notations, consider equivalent recursive sequence:

$$a_{n+1} = ka_n - a_{n-1} \qquad \text{where} \quad k = 2x_1$$

Also let the generating function be $f(t)$, then:

$$f(t) = a_0 + a_1 t + a_2 t^2 + a_3 t^3 + a_4 t^4 + \dots$$

Using the recursive formula we can rewrite $f(t)$ as:

$$f(t) = a_0 + a_1 t + (ka_1 - a_0)t^2 + (ka_2 - a_1)t^3 + (ka_3 - a_2)t^4 + \dots$$

We can regroup the terms as:

$$f(t) = a_0 + a_1 t + kt(a_1 t + a_2 t^2 + a_3 t^3 + \dots) - t^2(a_0 + a_1 t + a_2 t^2 + \dots)$$

Identify $f(t)$ in right hand side:

$$f(t) = a_0 + a_1 t + kt[f(t) - a_0] - t^2 f(t)$$

Isolate $f(t)$ on left hand side to get our generating function:

$$f(t) = \frac{a_0 + (a_1 - ka_0)t}{1 - kt + t^2} \tag{2.21}$$

Now to find n^{th} term we will express this generating function in partial fraction form:

$$\frac{a_0 + (a_1 - ka_0)t}{1 - kt + t^2} = \frac{a_0 + (a_1 - ka_0)t}{(1-\alpha t)(1-\beta t)} = \frac{A}{(1-\alpha t)} + \frac{B}{(1-\beta t)} \qquad \text{where} \quad \alpha, \beta \text{ are roots of } 1 - kt + t^2 \tag{2.22}$$

Using our quadratic equation root formula we get:

$$\alpha = \frac{k + \sqrt{k^2 - 4}}{2}, \qquad \beta = \frac{k - \sqrt{k^2 - 4}}{2}$$

Following standard method of finding partial fractions by comparing coefficients we get:

$$A = \frac{a_0(\alpha - k) + a_1}{\alpha - \beta}, \qquad B = \frac{a_0(\beta - k) + a_1}{\beta - \alpha}$$

Note that:

$$\frac{1}{1 - \alpha t} = 1 + \alpha t + \alpha^2 t^2 + \dots \quad \text{for } |\alpha t| < 1$$
$$\frac{1}{1 - \beta t} = 1 + \beta t + \beta^2 t^2 + \dots \quad \text{for } |\beta t| < 1$$

Substitute this in (2.22) to get:

$$f(t) = (A + B) + (A\alpha + B\beta)t + (A\alpha^2 + B\beta^2)t^2 + (A\alpha^3 + B\beta^3)t^3 \dots$$

Hence:

$$a_n = A\alpha^n + B\beta^n \tag{2.23}$$

Now substitute values A and B in this to get:

$$a_n = \frac{a_0(\alpha - k) + a_1}{\alpha - \beta}\alpha^n - \frac{a_0(\beta - k) + a_1}{\alpha - \beta}\beta^n$$

Further substitute the value of α and β to get:

$$a_n = \frac{a_0(-k + \sqrt{k^2 - 4}) + 2a_1}{2\sqrt{k^2 - 4}}\left(\frac{k + \sqrt{k^2 - 4}}{2}\right)^n - \frac{a_0(-k - \sqrt{k^2 - 4}) + 2a_1}{2\sqrt{k^2 - 4}}\left(\frac{k - \sqrt{k^2 - 4}}{2}\right)^n$$

But $k = 2x_1$, so we can simplify above expression to get:

$$a_n = \frac{a_0(-x_1 + \sqrt{x_1^2 - 1}) + a_1}{2\sqrt{x_1^2 - 1}} \left(x_1 + \sqrt{x_1^2 - 1}\right)^n - \frac{a_0(-x_1 - \sqrt{x_1^2 - 1}) + a_1}{2\sqrt{x_1^2 - 1}} \left(x_1 - \sqrt{x_1^2 - 1}\right)^n$$

Also, $x_1^2 - Dy_1^2 = 1$, so we can further simplify it as:

$$a_n = \frac{a_0(-x_1 + y_1\sqrt{D}) + a_1}{2y_1\sqrt{D}} \left(x_1 + y_1\sqrt{D}\right)^n - \frac{a_0(-x_1 - y_1\sqrt{D}) + a_1}{2y_1\sqrt{D}} \left(x_1 - y_1\sqrt{D}\right)^n$$

Now we can separate out x_n and y_n from this general case:

$$\begin{cases} x_n = \frac{x_0(-x_1+y_1\sqrt{D})+x_1}{2y_1\sqrt{D}} \left(x_1 + y_1\sqrt{D}\right)^n - \frac{x_0(-x_1-y_1\sqrt{D})+x_1}{2y_1\sqrt{D}} \left(x_1 - y_1\sqrt{D}\right)^n \\ y_n = \frac{y_0(x_1+1+y_1\sqrt{D})+y_1}{2y_1\sqrt{D}} \left(x_1 + y_1\sqrt{D}\right)^n - \frac{y_0(x_1+1-y_1\sqrt{D})+y_1}{2y_1\sqrt{D}} \left(x_1 - y_1\sqrt{D}\right)^n \end{cases}$$

Further, $x_0 = 1$ and $y_0 = 0$ thus finally we get:

$$\begin{cases} x_n = \frac{1}{2}[(x_1 + y_1\sqrt{D})^n + (x_1 - y_1\sqrt{D})^n] \\ y_n = \frac{1}{2\sqrt{D}}[(x_1 + y_1\sqrt{D})^n - (x_1 - y_1\sqrt{D})^n] \end{cases} \tag{2.24}$$

□

Methods to find particular solution. Finding an efficient method is a topic of research. The main method of determining the fundamental solution to such equations involves continued fractions [based on same idea as used in proof of *part (i)*].

We can write $\sqrt{D}$ in continued fraction form as:

$$\sqrt{D} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_1 + \cfrac{\ddots}{2q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots}}}}}$$

Because any continued fraction for $\sqrt{N}$ is necessarily of the form:

$$q_0, \underbrace{\overline{q_1, q_2, \ldots, q_2, q_1, 2q_0}}_{n \quad terms}$$

where the period begins immediately after the first term q_0 , and it consists of a symmetrical part $q_1, q_2, \ldots, q_2, q_1$, followed by the number $2q_0$ (for proof see pp. 92 of [15]).

Then the least solution to this equation turns out to be:

$$(x_1, y_1) = \begin{cases} (P_n, Q_n) & \text{if } n \quad \text{is even} \\ (P_{2n}, Q_{2n}) & \text{if } n \quad \text{is odd} \end{cases} \tag{2.25}$$

where $\frac{P_k}{Q_k} = \delta_k$ is k^{th} convergent of the continued fraction and $\delta_1 = q_0$.

Example 2.2.1. *Find the set of solutions for:*

a. $x^2 - 13y^2 = 1$

b. $x^2 - 21y^2 = 1$

Solution. a.

$$\sqrt{13} = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{\ddots}}}}}}$$

Hence here, $n = 5$, thus least solution is, (P_{10}, Q_{10}).

$$\delta_{10} = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}}}}}}} = \frac{649}{180} = \frac{P_{10}}{Q_{10}}$$

Indeed with a pocket calculator you can check that: $649^2 - 13(180)^2 = 1$
Hence the set of solutions is:

$$\begin{cases} x_n = \frac{1}{2}[(649 + 180\sqrt{13})^n + (649 - 180\sqrt{13})^n] \\ y_n = \frac{1}{2\sqrt{13}}[(649 + 180\sqrt{13})^n - (649 - 180\sqrt{13})^n] \end{cases}$$

b.

$$\sqrt{21} = 4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{8 + \cfrac{1}{\ddots}}}}}}}$$

Hence here, $n = 6$, thus the least solution is, (P_6, Q_6).

$$\delta_6 = 4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1}}}}} = \frac{55}{12} = \frac{P_6}{Q_6}$$

Again with a pocket calculator you can check that: $55^2 - 21(12)^2 = 1$
Thus the set of solutions is:

$$\begin{cases} x_n = \frac{1}{2}[(55 + 12\sqrt{21})^n + (55 - 12\sqrt{21})^n] \\ y_n = \frac{1}{2\sqrt{21}}[(55 + 12\sqrt{21})^n - (55 - 12\sqrt{21})^n] \end{cases}$$

Remark: The method of finding solutions by using continued fractions can even be extended to equations of form: $ax^2 - by^2 = c$, see [12]

2.2.2 Equations of form: $ax^2 - by^2 = 1$, $a, b \in \mathbb{Z}^+$

Consider the diophantine quadratic equation:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

with integral coefficients a, b, c, d, e, f. This equation represents a conic in the Cartesian plane, so solving this equation in integers means finding all lattice points situated on this conic. We can solve this equation in integers by reducing the general equation of the conic to its canonical form. Call the discriminant[6] of this equation $\triangle = b^2 - 4ac$.

---

[6] The discriminant of a quadratic form (a, b, c) is defined to be number $b^2 - 4ac$. It is an important fact that equivalent forms have the same discriminant. For more details see pp. 120 of [15]

1. When $\triangle < 0$, the conic defined by this equation is an ellipse, and in this case the given equation has only a finite number of solutions.
2. When $\triangle = 0$, the conic given by this equation is a parabola.
   (a) if $2ae - bd = 0$, given equation becomes $(2ax + by + d)^2 = d^2 - 4af$, which is easy to solve.
   (b) if $2ae-bd \neq 0$, by performing the substitutions $X = 2ax+by+d$ and $Y = (4ae-2bd)y+4af-d^2$, given equation reduces to $X^2 + Y = 0$, which is also easy to solve.
3. When $\triangle > 0$, when the conic defined by given equation is a hyperbola. Using a sequence of substitutions, given equation reduces to $x^2 - Dy^2 = A$, which is difficult to solve if $k = 1, D \in \mathbb{Z}^+$ and $\sqrt{D}$ is irrational (as seen in last subsection), else it is easier to solve.

Now consider the equation of type:

$$ax^2 - by^2 = 1, \qquad a, b \in \mathbb{Z}^+$$

Note that, in this case $\triangle > 0$, hence we may be able to reduce it to form: $x^2 - Dy^2 = 1$, $D \in \mathbb{Z}^+$ and $\sqrt{D}$ is irrational.

Theorem 2.2.2. *Given equation:*

$$ax^2 - by^2 = 1, \qquad a, b \in \mathbb{Z}^+$$

i. If $ab = k^2$, where $k \in \mathbb{Z}, k > 1$, then this equation does not have solutions in positive integers.

ii. Suppose that this equation has solutions in positive integers and let (x_1, y_1) be its minimal solution, i.e., the one with the least $y_1 > 0$. The general solution to this equation is $(x_n, y_n), n \geq 1$, where:

$$\begin{cases} x_n = by_1v_n - x_1u_n \\ y_n = ax_1v_n - y_1u_n \end{cases}$$

and $(u_n, v_n), n \geq 1$ is the non-trivial solution to $u^2 - abv^2 = 1$, $ab \in \mathbb{Z}^+$ and $\sqrt{ab}$ is irrational.

iii. In case of solvability of given equation, the relation between the fundamental solution (u_1, v_1) to $u^2 - abv^2 = 1$, $ab \in \mathbb{Z}^+$ and $\sqrt{ab}$ is irrational and the minimal solution (x_1, y_1) to given equation is :

$$u_1 \pm v_1\sqrt{ab} = \left(x_1\sqrt{a} \pm y_1\sqrt{b}\right)^2$$

where the signs $+$ and $-$ correspond.

iv. If (x_1, y_1) is the least solution of the equation then any solution of the equation is of form $(\pm x_n, \pm y_n)$,where

$$\begin{cases} x_n = \frac{-1}{2\sqrt{a}}\left[\left(x_1\sqrt{a} + y_1\sqrt{b}\right)^{2n-1} + \left(x_1\sqrt{a} - y_1\sqrt{b}\right)^{2n-1}\right] \\ y_n = \frac{1}{2\sqrt{b}}\left[\left(x_1\sqrt{a} + y_1\sqrt{b}\right)^{2n-1} - \left(x_1\sqrt{a} - y_1\sqrt{b}\right)^{2n-1}\right] \end{cases}$$

Proof. The main ideas of proof are based on previous theorem

i. Assume that given equation has a solution (α, β), where $\alpha, \beta \in \mathbb{Z}^+$. Then

$$a\alpha^2 - b\beta^2 = 1$$

and clearly α and β are relatively prime. From the condition $ab = k^2$ it follows that $a = k_1^2$ and $b = k_2^2$ for some positive integers k_1 and k_2 . Then the relation becomes:

$$k_1^2\alpha^2 - k_2^2\beta^2 = 1$$

can be written as

$$(k_1\alpha - k_2\beta)(k_1\alpha + k_2\beta) = 1$$

It follows that

$$1 < k_1\alpha + k_2\beta = k_1\alpha - k_2\beta = 1$$

a contradiction.

ii. Firstly verify that (x_n, y_n) is a solution to given equation. Indeed,

$$ax_n^2 - by_n^2 = a(by_1v_n - x_1u_n)^2 - b(ax_1v_n - y_1u_n)^2$$
$$\Rightarrow ax_n^2 - by_n^2 = (ax_1^2 - by_1^2)(u_n^2 - abv_n^2) = 1 \times 1 = 1$$

Conversely, let (x, y) be a solution to given equation.
Then note that (u, v), is a solution to $u^2 - abv^2 = 1$, $ab \in \mathbb{Z}^+$ and $\sqrt{ab}$ is irrational if,

$$\begin{cases} u = ax_1x + by_1y \\ v = y_1x + x_1y \end{cases}$$

Solving the above system of linear equations with unknowns x and y yields

$$\begin{cases} x = by_1v - x_1u \\ y = ax_1v - y_1u \end{cases}$$

Hence in general:

$$\begin{cases} x_n = by_1v_n - x_1u_n \\ y_n = ax_1v_n - y_1u_n \end{cases}$$

iii. Observe that:

$$\left(x_1\sqrt{a} \pm y_1\sqrt{b}\right)^2 = ax_1^2 + by_1^2 \pm 2x_1y_1\sqrt{ab}$$

But as observed in previous part:

$$\begin{cases} u_n = ax_1x_n + by_1y_n \\ v_n = y_1x_n + x_1y_n \end{cases}$$

Thus for $n = 1$,

$$\left(x_1\sqrt{a} \pm y_1\sqrt{b}\right)^2 = u_1 \pm v_1\sqrt{ab}$$

iv. We have already proved in previous parts of this theorem that:

$$\begin{cases} x_n = by_1v_n - x_1u_n \\ y_n = ax_1v_n - y_1u_n \end{cases} \qquad \text{and} \qquad \left(x_1\sqrt{a} \pm y_1\sqrt{b}\right)^2 = u_1 \pm v_1\sqrt{ab}$$

Further from (2.24) we know that:

$$\begin{cases} u_n = \frac{1}{2}[(u_1 + v_1\sqrt{ab})^n + (u_1 - v_1\sqrt{ab})^n] \\ v_n = \frac{1}{2\sqrt{ab}}[(u_1 + v_1\sqrt{ab})^n - (u_1 - v_1\sqrt{ab})^n] \end{cases}$$

Combining all these three results we get:

$$\begin{cases} x_n = by_1\left(\frac{1}{2\sqrt{ab}}\left[\left(x_1\sqrt{a} + y_1\sqrt{b}\right)^{2n} - \left(x_1\sqrt{a} - y_1\sqrt{b}\right)^{2n}\right]\right) - x_1\left(\frac{1}{2}\left[\left(x_1\sqrt{a} + y_1\sqrt{b}\right)^{2n} + \left(x_1\sqrt{a} - y_1\sqrt{b}\right)^{2n}\right]\right) \\ y_n = ax_1\left(\frac{1}{2\sqrt{ab}}\left[\left(x_1\sqrt{a} + y_1\sqrt{b}\right)^{2n} - \left(x_1\sqrt{a} - y_1\sqrt{b}\right)^{2n}\right]\right) - y_1\left(\frac{1}{2}\left[\left(x_1\sqrt{a} + y_1\sqrt{b}\right)^{2n} + \left(x_1\sqrt{a} - y_1\sqrt{b}\right)^{2n}\right]\right) \end{cases}$$

On combining similar terms we get:

$$\begin{cases} x_n = \frac{-1}{2\sqrt{a}}\left[\left(x_1\sqrt{a} - y_1\sqrt{b}\right)\left(x_1\sqrt{a} + y_1\sqrt{b}\right)^{2n} + \left(x_1\sqrt{a} + y_1\sqrt{b}\right)\left(x_1\sqrt{a} - y_1\sqrt{b}\right)^{2n}\right] \\ y_n = \frac{1}{2\sqrt{b}}\left[\left(x_1\sqrt{a} - y_1\sqrt{b}\right)\left(x_1\sqrt{a} + y_1\sqrt{b}\right)^{2n} - \left(x_1\sqrt{a} + y_1\sqrt{b}\right)\left(x_1\sqrt{a} - y_1\sqrt{b}\right)^{2n}\right] \end{cases}$$

But, $(x_1\sqrt{a} + y_1\sqrt{b})(x_1\sqrt{a} - y_1\sqrt{b}) = 1$, thus above expression further simplifies to:

$$\begin{cases} x_n = \frac{-1}{2\sqrt{a}}\left[\left(x_1\sqrt{a} + y_1\sqrt{b}\right)^{2n-1} + \left(x_1\sqrt{a} - y_1\sqrt{b}\right)^{2n-1}\right] \\ y_n = \frac{1}{2\sqrt{b}}\left[\left(x_1\sqrt{a} + y_1\sqrt{b}\right)^{2n-1} - \left(x_1\sqrt{a} - y_1\sqrt{b}\right)^{2n-1}\right] \end{cases}$$

$\square$

Methods to find particular solution. We are given following equation:

$$ax^2 - by^2 = 1$$

where $a, b \in \mathbb{Z}^+$ and $\sqrt{ab}$ is irrational. From this we will construct following equation:

$$u^2 - \sqrt{ab}v^2 = 1$$

where, $\sqrt{ab}$ is irrational.
Then find the least solution of our constructed equation by using continued fraction method. Further use the result proved above:

$$u_1 \pm v_1\sqrt{ab} = \left(x_1\sqrt{a} \pm y_1\sqrt{b}\right)^2$$

where $u_1, v_1 \in \mathbb{Z}^+$ is least solution of constructed equation and (x_1, y_1) is least solution of given equation. Thus, solution to given equation in $\mathbb{Z}^+$ exist if and only if we can find $x_1, y_1 \in \mathbb{Z}^+$ such that[7]

$$\begin{cases} u_1 = ax_1^2 + by_1^2 \\ v_1 = 2x_1y_1 \\ ax_1^2 - by_1^2 = 1 \end{cases}$$

So we have to solve another set of degree two diophantine equations in two variables. But since these are simultaneous equations these are easier to solve.

Example 2.2.2. *Solve in positive integers the equation:*

a. $6x^2 - 5y^2 = 1$

b. $5x^2 - 6y^2 = 1$

Solution. Note that for both given equations we will get same constructed equation:

$$u^2 - \sqrt{30}v^2 = 1$$

Now,

$$\sqrt{30} = 5 + \cfrac{1}{2 + \cfrac{1}{10 + \cfrac{1}{\ddots}}}$$

Since $n = 2$, thus least solution of this equation is (P_2, Q_2):

$$\delta_2 = 5 + \frac{1}{2} = \frac{11}{2} = \frac{P_2}{Q_2}$$

Thus, $u_1 = 11, v_1 = 2$. Now we need to validate:

$$\begin{cases} 11 = ax_1^2 + by_1^2 \\ 2 = 2x_1y_1 \\ 1 = ax_1^2 - by_1^2 \end{cases}$$

for each part.

a.

$$\begin{cases} 11 = 6x_1^2 + 5y_1^2 \\ 2 = 2x_1y_1 \\ 1 = 6x_1^2 - 5y_1^2 \end{cases}$$

On solving we get: $x_1 = 1, y_1 = 1$ as least solution, thus general solution of given equation is of form:

$$\begin{cases} x_n = \frac{-1}{2\sqrt{6}}\left[\left(\sqrt{6}+\sqrt{5}\right)^{2n-1} + \left(\sqrt{6}-\sqrt{5}\right)^{2n-1}\right] \\ y_n = \frac{1}{2\sqrt{5}}\left[\left(\sqrt{6}+\sqrt{5}\right)^{2n-1} - \left(\sqrt{6}-\sqrt{5}\right)^{2n-1}\right] \end{cases}$$

---

[7] There is a classic paper on this equation by D. T. Walker certainly worth peeping, refer [4].

b.

$$\begin{cases} 11 = 5x_1^2 + 6y_1^2 \\ 2 = 2x_1y_1 \\ 1 = 5x_1^2 - 6y_1^2 \end{cases}$$

On solving these simultaneous equations we get: $10x_1^2 = 12$ but $x_1 \in \mathbb{Z}$, thus given equation has *No Solution* in positive integers.

2.3 Equations of second degree in three unknowns

2.3.1 Pythagorean Triangles

Let's following theorem from geometry:

The length of radius of a circle inscribed in a Pythagorean Triangle is always an integer.

There would seem to be insufficient connection between the radius and sides to ensure that if the sides are integer, so is the radius. The proof is easy. But, to prove this you first need to have a parametric form for sides of triangle which is stated in following theorem.[8]

Theorem 2.3.1. *Any primitive solution*[9] (x, y, z) *in positive integers to*

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

with y*being an even number is of form:*

$$\begin{cases} x = m^2 - n^2 \\ y = 2mn \\ z = m^2 + n^2 \end{cases}$$

with m *and* n *are relatively prime positive integers with* $m > n$ *and* $m + n$ *is an odd number.*

Sketch of Proof. .

Method 1: This theorem is classic example of application of *Parametrization.* Rewrite given equation as:

$$y^2 = z^2 - x^2 = (z - x)(z + x)$$

Then use the fact that: *the product of two relatively prime numbers is a perfect square only if each factor is a perfect square.* Now consider parity argument to find parametric form of z and x.

Method 2: See Example 1.7.1 for proof using Unique Factorization Domain

Remark: Also the equations of form $x^2 + y^2 = az^2$ where $a \in \mathbb{Z}$ are not always solvable. But they can be easily dealt with modular arithmetic method.

2.3.2 Equations of form: $ax^2 + by^2 = z^2$, $a, b \in \mathbb{Z}^+$ and are square-free

Theorem 2.3.2. *The equation:*

$$ax^2 + by^2 = z^2$$

where $a, b \in \mathbb{Z}^+$ *and are square-free,*[10] *is solvable in integers if and only if following congruences are solvable*[11]

$$\begin{cases} a \equiv \alpha^2 \pmod{b}, & \text{where } \alpha = x'z, \quad xx' \equiv 1 \pmod{b} \\ b \equiv \beta^2 \pmod{a}, & \text{where } \beta \in \mathbb{Z} \\ a_1b_1 \equiv -\gamma^2 \pmod{h}, & \text{where } \gamma \in \mathbb{Z}, \quad h = \gcd(a, b), \quad a = ha_1, \quad b = hb_1 \end{cases}$$

Also, a_1*,* b_1*,* h *are relatively prime in pairs.*

---

[8] For proof of this theorem you just need to equate area of whole triangle with the sum of three smaller triangles (with radius as height). For whole proof refer pp. 68 of [2]

[9] A solution (x_0, y_0, z_0) to $x^2 + y^2 = z^2$ with x_0, y_0, z_0 relatively prime is called *primitive solution.*

[10] A number is called square-free if it is not divisible by any square greater than 1

[11] Notice that we need to deal only with square free numbers since for the introduction of square factors into the coefficients a and b does not affect the solvability of the equation.

Proof. We will consider three cases:

Case 1: If either a or b is 1, the equation is obviously soluble.[12]

Case 2: If $a = b$, the congruence conditions

$$\begin{cases} a \equiv \alpha^2 \pmod{b}, \\ b \equiv \beta^2 \pmod{a} \end{cases}$$

are trivially satisfied, and

$$a_1 b_1 \equiv -\gamma^2 \pmod{h},$$

reduces to:

$$1 \equiv -\gamma^2 \pmod{a}$$

Further[13], this implies that a is representable as $p^2 + q^2$, and the equation is satisfied by

$$\begin{cases} x = p, \\ y = q, \\ z = p^2 + q^2 \end{cases}$$

Case 3: Now suppose that $a > b > 1$.
By hypothesis, the congruence $b \equiv \beta^2 \pmod{a}$ is solvable. Choose a solution β which satisfies $|\beta| \leq \frac{a}{2}$. Since $\beta^2 - b$ is a multiple of a, we can put:

$$\beta^2 - b = aAk^2 \tag{2.26}$$

where k and A are integers and A is square free (all the square factors being absorbed in k^2). Note that k is relatively prime to b, since b is square free. We observe that A is positive:

$$aAk^2 = \beta^2 - b > -b > -a \quad \Rightarrow Ak^2 \geq 0 \quad \Rightarrow A > 0$$

since b is not a perfect square.
Now substitute y and z in terms of new variables Y and Z :

$$\begin{cases} z = bY + \beta Z, \\ y = \beta Y + Z, \end{cases}$$

because this substitution allows following manipulation:

$$(\beta - \sqrt{b})(Z - Y\sqrt{b}) = z - y\sqrt{b}$$

Moreover using this in given equation we get:

$$ax^2 = z^2 - by^2 = (\beta^2 - b)(Z^2 - bY^2)$$

Now using (2.26) we get:

$$ax^2 = aAk^2(Z^2 - bY^2)$$

Put, $x = kAX$ to get:

$$AX^2 + bY^2 = Z^2$$

If this equation is soluble, so is given equation.(Since the substitutions done above give integral values, not all zero, for x, y, z in terms of X, Y, Z)
The new coefficient A is positive and square free, and satisfies:

$$A = \frac{\beta^2 - b}{ak^2} < \frac{\beta^2}{ak^2} \leq \frac{\beta^2}{a} \leq \frac{a}{4} \quad \Rightarrow A < a$$

---

[12] Equations of form: $ax^2 + y^2 = z^2$ or $x^2 + ay^2 = z^2$, $a \in \mathbb{Z}$ can be solved by parametrization method, as an illustration see Example 1.3.1

[13] The congruence, $x^2 \equiv -1 \pmod{n}$ is solvable if and only if n has no prime factor of form $4k + 3$ and is also not divisible by 4. This, then is the necessary and sufficient condition for n to be properly representable as sum of two squares. For proof refer [15].

since we had assumed $|\beta| \leq \frac{a}{2}$
Now we will prove that A and b satisfy the congruence conditions analogous to the three given. By (2.26) we get :

$$b \equiv \beta^2 \pmod{A}$$

which is analogous equation of $b \equiv \beta^2 \pmod{a}$.
We can divide (2.26) by h, to get:

$$\frac{\beta^2}{h} - \frac{b}{h} = \frac{a}{h}Ak^2$$

But we are given that: $a = ha_1$ and $b = hb_1$, also let: $\beta = h\beta_1$, then we get:

$$h\beta_1^2 - b_1 = a_1Ak^2 \quad \Rightarrow h\beta_1^2 \equiv a_1Ak^2 \pmod{b_1} \tag{2.27}$$

Similarly if we let, $\alpha = h\alpha_1$, then $a \equiv \alpha^2 \pmod{b}$ is equivalent to $a \equiv h^2\alpha_1^2 \pmod{b}$, but again given that $a = ha_1$ and $b = hb_1$, we obtain:

$$a_1 \equiv h\alpha_1^2 \pmod{b_1} \tag{2.28}$$

Now combining (2.27) and (2.28), we get:

$$h\beta_1^2 \equiv hA(k\alpha_1)^2 \pmod{b_1}$$

and since h, k, a_1 are all relatively prime to b_1 it follows that A is congruent to a square $\pmod{b_1}$. and in view of $a_1b_1 \equiv -\gamma^2 \pmod{h}$ and the fact that k, a_1, b_1 are all relatively prime to h it follows that A is congruent to a square $\pmod{h}$, and therefore also $\pmod{b}$, giving the analogue of $a \equiv \alpha^2 \pmod{b}$.
Let H denote the highest common factor of A and b, and put $A = HA_2$, $b = Hb_2$. The equation (2.26) can be divided by H , giving:

$$H\beta_2^2 - b_2 = aA_2k^2$$

Multiply by A_2 to get:

$$-A_2b_2 \equiv a(A_2k)^2 \pmod{H}$$

Also,[14]

$$a \equiv \alpha^2 \pmod{b} \quad \Rightarrow a \equiv \alpha^2 \pmod{Hb_2} \quad \Rightarrow a \equiv \alpha^2 \pmod{H}$$

it follows that $-A_2b_2$ is congruent to a square $\pmod{H}$, which is the analogue of $a_1b_1 \equiv -\gamma^2 \pmod{h}$. We have derived from given equation a similar equation with the same b but with a replaced by A, where $0 < A < a$, and A, b satisfy the same three congruence conditions as a, b. Repetition of the process must lead eventually to an equation in which either one coefficient is 1 or the two coefficients are equal. As we have seen, such an equation is soluble.

□

Methods to find particular solution. We may follow Law of Quadratic Reciprocity to solve the congruences (if exist) if a and b are prime. Then to find solutions follow the procedure illustrated in proof above.

Example 2.3.1. *Solve the equation* $41x^2 + 31y^2 = z^2$ *in positive integers.*

Solution. Since the coefficients are relatively prime, there are only the two congruence conditions:

$$\begin{cases} 41 \equiv \alpha^2 \pmod{31}, \\ 31 \equiv \beta^2 \pmod{41} \end{cases}$$

Method 1: Since $41 \equiv 1 \pmod{4}$ and $31 \equiv 3 \pmod{4}$, by Law of Quadratic Reciprocity:

$$\left(\frac{31}{41}\right) = \left(\frac{41}{31}\right) = \left(\frac{10}{31}\right) = \left(\frac{2}{31}\right)\left(\frac{5}{31}\right) = \left(\frac{2}{31}\right)\left(\frac{31}{5}\right) = \left(\frac{2}{31}\right)\left(\frac{1}{5}\right) = \left(\frac{2}{31}\right) = 1$$

Since, $8^2 \equiv 2 \pmod{31}$. Hence both of these congruences are solvable.

---

[14] For example, since, $9 \equiv 3 \pmod{6} \quad \Rightarrow 9 \equiv 3 \pmod{2} \quad \& \quad 9 \equiv 3 \pmod{3}$, though they are not in their lowest form.

Method 2: If you don't know Law of Quadratic reciprocity, then you will have to solve equation and check (also if a and b would not have been prime):

$$\alpha^2 \equiv 41 \pmod{31} \quad \Rightarrow \alpha^2 \equiv 10 \pmod{31}$$

Firstly we will calculate Phi Function: $\phi(31) = 30$ then since: $\gcd(41, 31) = 1$ and $\gcd(2, 30) \neq 1$ thus we can't use our standard method of computing k^{th} roots modulo m. Thus I will have to generate a table till I get 10 as residue (maximum upto $\alpha = \frac{31-1}{2} = 15$)

α	1	2	3	4	5	6	7	8	9	10	11	12	13	14
α^2	1	4	9	16	25	36	49	64	81	100	121	144	169	196
mod 31	1	4	9	16	25	5	18	2	19	7	28	20	14	10

Thus $\alpha = 14$ is a solution, and by symmetry, $\alpha = 31 - 14 = 17$.
Similarly I will have to generate a table for $\beta^2 \equiv 31 \pmod{41}$ till I get 31 as residue (maximum upto $\beta = \frac{41-1}{2} = 20$)

β	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
β^2	1	4	9	16	25	36	49	64	81	100	121	144	169	196	225	256	289	324	361	400
mod 41	1	4	9	16	25	36	8	23	40	18	39	21	5	32	20	10	2	37	33	31

Thus $\beta = 20$ is a solution, and by symmetry, $\beta = 41 - 20 = 21$.
Hence solution to given equation exist.

Now to find solutions we must choose a value for β and then define A and k as:

$$\beta^2 - b = aAk^2$$

As we did in proof, let: $|\beta| \leq \frac{a}{2}$, so we take $\beta = 20$, and have:

$$\beta^2 - b = 400 - 31 = 9 \times 41, \quad \Rightarrow k = 3, A = 1.$$

Note that, $A = 1$ means that no further repetition of the process will be necessary.
Now as did in proof we replace:

$$\begin{cases} z = 31Y + 20Z, \\ y = 20Y + Z, \\ x = 3X \end{cases}$$

Then the new equation derived from given equation is

$$X^2 + 31Y^2 = Z^2$$

This can be solved as in Example: 1.3.1:

$$31Y^2 = Z^2 - X^2 = (Z + X)(Z - X)$$

Now since LHS is an integer, so 31 will divide either $(Z - X)$ or $(Z + X)$, In the first case, if 31 divide $Z - X$

$$\begin{cases} Z + X = n^2, \\ Z - X = 31m^2 \\ Y = mn \end{cases}$$

while in second case:

$$\begin{cases} Z + X = 31m^2, \\ Z - X = n^2 \\ Y = mn \end{cases}$$

where n and m are positive integers
Solving these two systems of equations we get:

$$\begin{cases} X = \frac{n^2-31m^2}{2}, \\ Y = mn \\ Z = \frac{n^2+31m^2}{2} \end{cases} \quad or \quad \begin{cases} X = \frac{31m^2-n^2}{2}, \\ Y = mn \\ Z = \frac{n^2+31m^2}{2} \end{cases}$$

respectively.
Now combine above two expressions and get general parametric form as:

$$\begin{cases} X = \pm\frac{n^2-31m^2}{2}, \\ Y = mn \\ Z = \frac{n^2+31m^2}{2} \end{cases}$$

where m, n are even numbers.
From these we get x, y, z by reversing replacement as:

$$\begin{cases} x = \pm\frac{3(n^2-31m^2)}{2}, \\ y = \frac{n^2+40mn+31m^2}{2} \\ z = 10n^2 + 310m^2 + 31mn \end{cases}$$

where m, n are even numbers.
For example, for $m = 2, n = 2$ we get:

$$\begin{cases} x = 180 \\ y = 144 \\ z = 1404 \end{cases} \xrightarrow{\text{cancelling common factors}} \begin{cases} x = 5 \\ y = 4 \\ z = 39 \end{cases}$$

Thus this form will give infinite solutions but NOT all solutions, like: $(3, 1, 20)$.

2.3.3 Equations of form: $x^2 + axy + y^2 = z^2$, $a \in \mathbb{Z}$

The Pythagorean equation is a special case of this equation with $a = 0$.

Theorem 2.3.3. *All integral solutions to $x^2 + axy + y^2 = z^2$, $a \in \mathbb{Z}$ are given by:*

$$\begin{cases} x = k(ap^2 - 2pq), \\ y = k(q^2 - p^2), \\ z = \pm k(apq - p^2 - q^2) \end{cases} \qquad \begin{cases} x = k(q^2 - p^2), \\ y = k(ap^2 - 2pq) \\ z = \pm k(apq - p^2 - q^2) \end{cases}$$

where $p, q \in \mathbb{Z}$ are relatively prime and $k \in \mathbb{Q}$ such that $(a^2 - 4)k \in \mathbb{Z}$

Proof. Note that the two families of solutions follow symmetry of given equation in x and y.

Check by substituting these values of x, y, z in given equation.
Now we need to show that *all* solutions of given equation are of given form. Given equation is equivalent to:

$$x(x + ay) = (z - y)(z + y)$$

We can rewrite this as:

$$\frac{x}{z-y} = \frac{z+y}{x+ay}$$

Now let, p, q are integers and $\gcd(q, p) = 1$. Then, $\frac{p}{q}$ be the corresponding irreducible fraction, we get:

$$\frac{x}{z-y} = \frac{z+y}{x+ay} = \frac{p}{q}$$

From this we get:

$$\begin{cases} qx = p(z-y) \\ q(z+y) = p(x+ay) \end{cases} \Rightarrow \begin{cases} qx + py - pz = 0 \\ px + (pa-q)y - qz = 0 \end{cases}$$

Now from these simultaneous equations we can get x and y in terms of z as:

$$\begin{cases} x = \dfrac{(ap^2 - 2pq)z}{apq - p^2 - q^2} \\ y = \dfrac{(q^2 - p^2)z}{apq - p^2 - q^2} \end{cases}$$

Now choose $z = k(apq - p^2 - q^2), k \in \mathbb{Q}$ and get given solutions.
Further if, $k = \frac{r}{s}$ in lowest form, then:

$$s \Big| \gcd\left(ap^2 - 2pq, q^2 - p^2, apq - p^2 - q^2\right)$$

$$\Rightarrow s \Big| \left(a\left(ap^2 - 2pq\right) + 2\left(q^2 - p^2\right) + 2\left(apq - p^2 - q^2\right)\right)$$

$$\Rightarrow s \Big| \left(\left(a^2 - 4\right)p^2\right)$$

But:

$$s \Big| p^2 \quad \Rightarrow s \Big| p \quad \Rightarrow s \not\Big| (q^2 - p^2)$$

since p, q are relatively prime. Hence:

$$s \Big| (a^2 - 4)$$

Which is equivalent to:

$$(a^2 - 4)k \in \mathbb{Z}$$

□

2.3.4 Equations of form: $ax^2 + by^2 + cz^2 = 0; a, b, c, \in \mathbb{Z} \setminus \{0\}$ and abc is square-free

The general *Ternary Quadratic Form* is a polynomial $f(x, y, z)$ of form:

$$f(x, y, z) = ax^2 + by^2 + cz^2 + dxy + eyz + fzx.$$

A triple (x, y, z) of numbers for which $f(x, y, z) = 0$ is called a zero of the form. The solution $(0, 0, 0)$ is the trivial zero. Any *Ternary Quadratic Form* can be converted to $ax^2 + by^2 + cz^2 = 0; a, b, c, \in \mathbb{Z} \setminus \{0\}$ by doing appropriate substitutions and transformations.[15]

Theorem 2.3.4. *Let a, b, c be non-zero integers such that the product abc is square-free. Necessary and sufficient conditions that $ax^2 + by^2 + cz^2 = 0$ have a non-trivial solution in integers x, y, z, are that:*

i. a, b, c do not have the same sign

ii. $-bc, -ac, -ab$ are quadratic residues modulo a, b, c, respectively.
Symbolically:

$$\begin{cases} -bc \equiv \alpha^2 \pmod{a} \\ -ac \equiv \beta^2 \pmod{b} \\ -ab \equiv \gamma^2 \pmod{c} \end{cases}$$

where $\alpha, \beta, \gamma \in \mathbb{Z}$, all three congruences are solvable.

Proof. i. If $ax^2 + by^2 + cz^2 = 0$, has a solution x_0, y_0, z_0 not all zero, then a, b, c are not of the same sign. Dividing x_0, y_0, z_0 by $\gcd(x_0, y_0, z_0)$ we have a solution x_1, y_1, z_1 with $\gcd(x_1, y_1, z_1) = 1$

---

[15] For more details refer pp. 246-248 of [9]

ii. Let $\gcd(x_1, c) = p$. Then $p \not| b$ since $p|c$ and abc is square-free. Therefore

$$p\big|by_1^2 \quad \Rightarrow p\big|y_1^2 \quad \Rightarrow p\big|y_1$$

and then,

$$p^2\big|(ax_1^2 + by_1^2) \quad \Rightarrow p^2\big|cz_1^2 \quad \Rightarrow p^2\big|z_1^2 \quad \Rightarrow p\big|z_1$$

since c is square-free.
Hence p is a factor of x_1, y_1, z_1 contrary to $\gcd(x_1, y_1, z_1) = 1$. Thus, we have $\gcd(c, x_1) = 1$.
Let u be chosen to satisfy:

$$ux_1 \equiv 1 \pmod{c} \tag{2.29}$$

The equation $ax_1^2 + by_1^2 + cz_1^2 = 0$ implies:

$$ax_1^2 + by_1^2 \equiv 0 \pmod{c}$$

Multiplying this by u^2b and using (2.29) we get:

$$u^2b^2y_1^2 \equiv -ab \pmod{c}$$

Thus we have established that $-ab$ is a quadratic residue modulo c.
A similar proof shows that $-bc$ and $-ac$ are quadratic residues modulo a and b respectively.

Conversely: Let us assume that $-bc, -ab - ca$ are quadratic residues modulo a, b, c respectively.
Note that this property does not change if a, b, c are replaced by their negatives. Since a, b, c are not of the same sign, we can change the signs of all of them, if necessary, in order to have one positive and two of them negative. Then, perhaps with a change of notation, we can arrange it so that a is positive and b and c are negative.
Define r as a solution of:

$$r^2 \equiv -ab \pmod{c} \tag{2.30}$$

and, a_1 as a solution of:

$$aa_1 \equiv 1 \pmod{c} \tag{2.31}$$

These solutions r and a_1 exist because of our assumptions on a, b, c. Then we can write previous equation as:

$$\Rightarrow ax^2 + by^2 \equiv aa_1(ax^2 + by^2) \equiv a_1(a^2x^2 + aby^2) \pmod{c}$$

Now using, (2.30), we get:

$$\Rightarrow ax^2 + by^2 \equiv a_1(a^2x^2 - r^2y^2) \pmod{c}$$

$$\Rightarrow ax^2 + by^2 \equiv a_1(ax - ry)(ax + ry) \pmod{c}$$

Using, (2.31) again, we get:

$$\Rightarrow ax^2 + by^2 \equiv (x - a_1ry)(ax + ry) \pmod{c}$$

Thus $ax^2 + by^2 + cz^2$ is the product of two linear factors modulo c, and similarly modulo a and modulo b.
Since $ax^2 + by^2 + cz^2$ factors into linear factors modulo c and also modulo a, and $\gcd(a, c) = 1$, thus $ax^2 + by^2 + cz^2$ also factors modulo ac as a consequence of *Chinese Remainder Theorem*[16].
Now, since $ax^2 + by^2 + cz^2$ factors into linear factors modulo b and also modulo ca, and $\gcd(ca, b) = 1$, thus $ax^2 + by^2 + cz^2$ also factors modulo abc, again as a consequence of *Chinese Remainder Theorem*.
Thus, there exist numbers $\alpha_1, \beta_1, \gamma_1, \alpha_2, \beta_2, \gamma_2$ such that:

$$ax^2 + by^2 + cz^2 \equiv \Big((\alpha_1x + \beta_1y + \gamma_1z)(\alpha_2x + \beta_2y + \gamma_2z)\Big) \pmod{abc} \tag{2.32}$$

Now consider the congruence:

$$(\alpha_1x + \beta_1y + \gamma_1z) \equiv 0 \pmod{abc} \tag{2.33}$$

---

[16] For proof see pp. 243 of [9]

Since, $a > 0; b, c < 0$, let $\lambda = \sqrt{bc}, \mu = \sqrt{|ac|}, \eta = \sqrt{|ab|}$.
Now, λ, μ, η are positive real numbers with product $\lambda\mu\eta = abc \in \mathbb{Z}$. Then,

$$(\alpha_1 x + \beta_1 y + \gamma_1 z) \equiv 0 \pmod{\lambda\mu\eta} \tag{2.34}$$

Let x range over the values $\{0, 1, \ldots, \lfloor\lambda\rfloor\}$, y over the values $\{0, 1, \ldots, \lfloor\mu\rfloor\}$, and z over the values $\{0, 1, \ldots, \lfloor\eta\rfloor\}$.
This gives us $(1 + \lfloor\lambda\rfloor)(1 + \lfloor\mu\rfloor)(1 + \lfloor\eta\rfloor)$ different triples x, y, z.
Now as per properties of floor function:

$$(1 + \lfloor\lambda\rfloor)(1 + \lfloor\mu\rfloor)(1 + \lfloor\eta\rfloor) > \lambda\mu\eta = abc$$

and hence there must be some two triples (x_1, y_1, z_1) and (x_2, y_2, z_2) such that:

$$\alpha_1 x_1 + \beta_1 y_1 + \gamma_1 z_1 \equiv \alpha_1 x_2 + \beta_1 y_2 + \gamma_1 z_2 \pmod{abc}$$

Then we have

$$\alpha_1(x_1 - x_2) + \beta_1(y_1 - y_2) + \gamma_1(z_1 - z_2) \equiv 0 \pmod{abc}$$

Thus,

$$\begin{cases} |x_1 - x_2| \le \lfloor\lambda\rfloor \le \lambda, \\ |y_1 - y_2| \le \lfloor\mu\rfloor \le \mu, \\ |z_1 - z_2| \le \lfloor\eta\rfloor \le \eta \end{cases}$$

Then the equation (2.33) [which is equivalent to (2.34)] has a solution x_1, y_1, z_1, not all zero, such that

$$\begin{cases} |x_1| \le \lambda, \\ |y_1| \le \mu, \\ |z_1| \le \eta \end{cases} \Rightarrow \begin{cases} |x_1| \le \sqrt{bc}, \\ |y_1| \le \sqrt{|ac|}, \\ |z_1| \le \sqrt{|ab|} \end{cases}$$

But abc is square-free, so $\sqrt{bc}$ is an integer only if it is 1, and similarly for $\sqrt{|ac|}$ and $\sqrt{|ab|}$. Therefore:

$$\begin{cases} x_1^2 \le bc, & \text{equality possible only if } b = c = -1 \\ y_1^2 \le -ac, & \text{equality possible only if } a = 1, c = -1 \\ z_1^2 \le -ab, & \text{equality possible only if } a = 1, b = -1 \end{cases}$$

Hence, since a is positive and b and c are negative, we have, unless $b = c = 1$,

$$ax_1^2 + by_1^2 + cz_1^2 \le ax_1^2 < abc$$

and

$$ax_1^2 + by_1^2 + cz_1^2 \ge by_1^2 + cz_1^2 > b(-ac) + c(-ab) = -2abc$$

Leaving aside the special case when $b = c = -1$, we have:

$$-2abc < ax_1^2 + by_1^2 + cz_1^2 < abc$$

Now (x_1, y_1, z_1) is a solution of (2.33) and so also, because of (2.32), a solution of :

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{abc}$$

Thus the above inequalities imply that:

$$ax_1^2 + by_1^2 + cz_1^2 = 0 \qquad \text{or} \qquad ax_1^2 + by_1^2 + cz_1^2 = -abc$$

In the first case we have our solution of given equation.
In the second case we verify that (x_2, y_2, z_2), defined by:

$$\begin{cases} x_2 = -by_1 + x_1 z_1, \\ y_2 = ax_1 + y_1 z_1, \\ z_2 = z_1^2 + ab, \end{cases}$$

form a solution. Also, if $x_2 = y_2 = z_2 = 0$, then

$$z_1^2 + ab = 0 \quad \Rightarrow z_1^2 \; = -ab \quad \Rightarrow z_1 = \pm 1$$

because ab, like abc, is square-free. Then $a = 1, b = 1$, and $x = 1, y = -1, z = 0$ is a solution.
Finally we dispose of the special case $b = c = -1$. The conditions on a, b, c now imply that -1 is a quadratic residue modulo a; in Legendre symbols,

$$\left(\frac{-1}{a}\right) = 1$$

This implies[17] that the equation $y^2 + z^2 = a$ has a solution y_1, z_1. Then $x = 1, y = y_1, z = z_1$ is a solution of given equation i.e. $ax^2 + by^2 + cz^2 = 0$ since $b = c = -1$.

Thus we have proved that given to us is necessary and sufficient condition. □

Methods to find particular solution. Here we will use the *geometry* to relate rational solutions to integer solutions. [as commented in "Introduction" of this report.]

- If we have a solution in rational numbers, not all zero, then we can construct a primitive solution in integers by multiplying each coordinate by the least common multiple of denominators of the three.
  ILLUSTRATION: Since $(\frac{3}{5}, \frac{4}{5}, 1)$ is a zero of the form $f(x, y, z) = x^2 + y^2 - z^2$, and hence $(3, 4, 5)$ is a primitive integral solution.

- All solutions of this equation may be found, once a single solution has been identified by using concept of *Rational Points on Curves*.
  ILLUSTRATION: In case of finding Pythagorean Triples (integer solutions of Pythagoras Theorem), finding non-trivial primitive i.e. pairwise relatively prime integer solutions of $X^2 + Y^2 - Z^2 = 0$ is equivalent to finding rational points on unit circle centred at origin i.e. $x^2 + y^2 = 1$ (a conic section), where $\frac{X}{Z} = x, \frac{Y}{Z} = y$. Every point on this circle whose coordinates are rational numbers can be obtained from the formula[18]

  $$(x, y) = \left(\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2}\right)$$

  by substituting in rational numbers for m [except for the point $(-1, 0)$ which is the limiting value as $m \to \infty$].
  If we replace $m = \frac{p}{q}$, we get the formula we derived in Section 2.3.1,

  $$\begin{cases} X = p^2 - q^2 \\ Y = 2pq \\ Z = p^2 + q^2 \end{cases}$$

- Thus we can reduce the problem of finding non-trivial primitive i.e. pairwise relatively prime integer solutions of $aX^2 + bY^2 + cZ^2$ to an equivalent problem of finding rational points on a conic section : $ax^2 + by^2 + c = 0$. Now this can be handled as discussed in Section: 2.2.2. [i.e depending upon type of conic section]

2.4 Equations of degree higher than the second in three unknowns

2.4.1 Equations of form: $x^4 + x^2y^2 + y^4 = z^2$

Theorem 2.4.1. *All non-negative integer solutions of the equation:*

$$x^4 + x^2y^2 + y^4 = z^2$$

---

[17] The congruence, $x^2 \equiv -1 \pmod{n}$ is solvable if and only if n has no prime factor of form $4k + 3$ and is also not divisible by 4. This, then is the necessary and sufficient condition for n to be properly representable as sum of two squares. For proof refer [15].

[18] For derivation refer pp. 21 of [16].

are given by:

$$\begin{cases} x = k \\ y = 0 \\ z = k^2 \end{cases} \qquad \begin{cases} x = 0 \\ y = k \\ z = k^2 \end{cases}$$

where $k \in \mathbb{Z}^+$.

Proof. Firstly, since right hand side of given equation is a perfect square, so left hand side, which is a symmetric quadratic in x and y should also satisfy, perfect square rule of a quadratic, i.e. discriminant w.r.t. both x^2 and y^2 should be zero.
With respect to x^2: $\Delta = y^4 - 4y^4 = 0 \quad \Rightarrow y = 0$, but this will be true for all x, since we have not imposed any condition on x, thus $(k, 0, k^2)$ is solution of this equation for all $k \in \mathbb{Z}^+$
With respect to y^2: $\Delta = x^4 - 4x^4 = 0 \quad \Rightarrow x = 0$, but this will be true for all y, since we have not imposed any condition on y, thus $(0, k, k^2)$ is solution of this equation for all $k \in \mathbb{Z}^+$
Also, by completing squares, given equation is equivalent to:

$$\left(x^2 - y^2\right)^2 + 2(xy)^2 = z^2$$

which eliminates the possibility of $x = y \neq 0$ as a solution. But we need to prove that these are the "only solutions".
Let, (x_1, y_1, z_1) be a solution to given equation. Assume that $\gcd(x_1, y_1) = 1$. Then x_1 and y_1 have different parities, for otherwise $z_1^2 \equiv 3 \pmod 4$. Suppose that $y_1 > 0$ is odd and minimal.
Multiply given equation by 4 and simplify:

$$\Rightarrow 4x_1^4 + 4x_1^2y_1^2 + 4y_1^4 = 4z_1^2$$

$$\Rightarrow 4z_1^2 - \left(2x_1^2 + y_1^2\right)^2 = 3y_1^4$$

$$\Rightarrow \left(2z_1 - 2x_1^2 - y_1^2\right)\left(2z_1 + 2x_1^2 + y_1^2\right) = 3y_1^4 \tag{2.35}$$

Now assume that d is a prime dividing both $2z_1 + 2x_1^2 + y_1^2$ and $2z_1 - 2x_1^2 - y_1^2$. Thus,

$$\gcd\left((2z_1 + 2x_1^2 + y_1^2), (2z_1 - 2x_1^2 - y_1^2)\right) = d$$

$$\Rightarrow d \Big| (2z_1 + 2x_1^2 + y_1^2)$$

Then d is odd,

$$\Rightarrow d \big| z_1 \quad \text{and} \quad d \big| (2x_1^2 + y_1^2)$$

From (2.35) it follows that $d \big| 3y_1$.
If $d > 3$, then $d \big| y_1$ and $d \big| 2x_1^2$, i.e., $\gcd(x_1, y_1) \geq d$, a contradiction.
If $d = 3$, it follows that $3 \big| z_1$, and from given equation we obtain $3 \big| (2x_1^2 + y_1^2)$, so $3 \big| y_1$. Therefore $3 \big| x_1$, and so $\gcd(x_1, y_1) \geq 3$, a contradiction.
Hence:

$$\gcd\left((2z_1 + 2x_1^2 + y_1^2), (2z_1 - 2x_1^2 - y_1^2)\right) = 1$$

Thus to satisfy (2.35),

$$\begin{cases} 2z_1 + 2x_1^2 + y_1^2 = a^4, \\ 2z_1 - 2x_1^2 - y_1^2 = 3b^4, \\ y_1 = ab \end{cases} \qquad \text{or} \qquad \begin{cases} 2z_1 + 2x_1^2 + y_1^2 = 3a^4, \\ 2z_1 - 2x_1^2 - y_1^2 = b^4, \\ y_1 = ab \end{cases}$$

where a and b are both odd positive integers.
In first case, on simplification we get:

$$4x_1^2 = a^4 - 2a^2b^2 - 3b^4 = (a^2 + b^2)(a^2 - 3b^2)$$

Now applying modulo arithmetic method, since fourth powers are involved we will consider modulo $2^4 = 16$, thus[19]:

$$a^4 - 2a^2b^2 - 3b^4 \equiv -4 \pmod{16}$$

Since a and b are both odd. But: $4x_1^2 \equiv 0 \pmod{16}$, since x_1 is even. Thus no value of (x_1, y_1, z_1) satisfy first case.

In second case, on simplification we get:

$$4x_1^2 = 3a^4 - 2a^2b^2 - b^4 = (a^2 - b^2)(3a^2 + b^2)$$

Further observe that[20] since a and b are both odd, it follows that

$$\begin{cases} a^2 - b^2 = c^2 \\ 3a^2 + b^2 = 4d^2 \end{cases}$$

where $c, d \in \mathbb{Z}$.

Now substitute:

$$\begin{cases} a = p^2 + q^2 \\ b = p^2 - q^2 \end{cases}$$

where $p, q \in \mathbb{Z}^+$, to get:

$$3(p^2 + q^2)^2 + (p^2 - q^2)^2 = 4p^4 + 4p^2q^2 + 4q^4 = 4d^2$$
$$\Rightarrow p^4 + p^2q^2 + q^4 = d^2$$

Which is equivalent to given equation, thus (p, q, d) and (q, p, d) is solution to give equation.

But, since $y_1 = ab$, thus $y_1 > a$. But, $a > p^2 > p; a > q^2 > q$, thus, $y_1 > p, q$. But this contradicts the minimality of y_1.

Thus, $y_1 = 0$ [minimal non-negative value], which implies, $z_1 = x_1^2$. Hence, $(k, 0, k^2)$ for $k \in \mathbb{Z}^+$. gives a solution.

By symmetry, other solution (by contradicting minimality of x_1) is $(0, k, k^2)$ for $k \in \mathbb{Z}$ □

2.4.2 Equations of form: $x^4 - x^2y^2 + y^4 = z^2$

Theorem 2.4.2. *All non-negative integer solutions of the equation:*

$$x^4 - x^2y^2 + y^4 = z^2$$

are given by:

$$\begin{cases} x = k \\ y = 0 \\ z = k^2 \end{cases} \quad \begin{cases} x = 0 \\ y = k \\ z = k^2 \end{cases} \quad \begin{cases} x = k \\ y = k \\ z = k^2 \end{cases}$$

where $k \in \mathbb{Z}^+$.

Proof. Given equation is equivalent to [Pythagoras equation form]:

$$\left(x^2 - y^2\right)^2 + (xy)^2 = z^2$$

Let (x_1, y_1, z_1) be solution of given equation. Assume that $\gcd(x_1, y_1) = 1$ and that $x_1y_1 > 0$ is minimal. We will consider two cases:

---

[19] For more details about selection of number with respect to which we should check residue refer Chapter-2 of [5].

[20] Modulo arithmetic method won't help here:

$$3a^4 - 2a^2b^2 - b^4 \equiv 0 \pmod{16}$$

Thus solution of this equation may or may not exist.

Case 1: *x_1 and y_1 are of different parity*

Then, for some positive integers a and b, with $\gcd(a, b) = 1$, let [Pythagorean Triple]:

$$\begin{cases} x_1^2 - y_1^2 = a^2 - b^2 \\ x_1 y_1 = 2ab \\ z_1 = a^2 + b^2 \end{cases} \tag{2.36}$$

Let, $\gcd(x_1, b) = d_1$ and $\gcd(y_1, a) = d_2$, then:

$$\begin{cases} x_1 = d_1 X_1, \\ b = d_1 B, \\ y_1 = d_2 Y_1, \\ a = d_2 A, \\ X_1 Y_1 = 2AB. \end{cases}$$

for some positive integers A, B, X_1, Y_1 such that $\gcd(X_1, B) = \gcd(Y_1, A) = 1$, thus:

$$\begin{cases} X_1 = 2A, \\ Y_1 = B \end{cases} \quad \text{or} \quad \begin{cases} X_1 = A, \\ Y_1 = 2B \end{cases}$$

hence giving respective set of values as:

$$\begin{cases} x_1 = 2d_1 A, \\ b = d_1 B, \\ y_1 = d_2 B, \\ a = d_2 A \end{cases} \quad \text{or} \quad \begin{cases} x_1 = d_1 A \\ b = d_1 B, \\ y_1 = 2d_2 B, \\ a = d_2 A \end{cases}$$

Now substituting the first set of values in (2.36) we get:

$$\begin{aligned} &\Rightarrow \left(2d_1 A\right)^2 - \left(d_2 B\right)^2 = \left(d_2 A\right)^2 - (d_1 B)^2 \\ &\Rightarrow d_1^2\left(4A^2 + B^2\right) = d_2^2\left(A^2 + B^2\right) \end{aligned} \tag{2.37}$$

Further:

$$\gcd(a, b) = 1 \quad \Rightarrow \gcd(A, B) = 1$$

Let, $\gcd\Big(\left(4A^2 + B^2\right), \left(A^2 + B^2\right)\Big) = d$, thus:

$$d \Big| \Big(\left(4A^2 + B^2\right) - \left(A^2 + B^2\right)\Big) \quad \Rightarrow d \big| 3A^2$$

But, for these set of values,

$$\gcd(X_1, B) = \gcd(2A, B) = 1 \quad \Rightarrow \gcd(A, B) = 1$$

thus,

$$3 \not| (A^2 + B^2) \quad \Rightarrow d \not| 3 \quad \Rightarrow d \big| A^2 \quad \Rightarrow d \big| A$$

Similarly,

$$d \Big| \Big(4\left(A^2 + B^2\right) - \left(4A^2 + B^2\right)\Big) \quad \Rightarrow d \big| 3B^2 \quad \Rightarrow d \big| B^2 \quad \Rightarrow d \big| B$$

By condition, $\gcd(A, B) = 1$ and $d \big| A$ and $d \big| B$ we get $d = 1$, thus

$$\gcd\Big(\left(4A^2 + B^2\right), \left(A^2 + B^2\right)\Big) = 1$$

Now in (2.37), we write two equations of second degree in three unknowns as:

$$\begin{cases} A^2 + B^2 = C^2 \\ 4A^2 + B^2 = D^2 \end{cases} \tag{2.38}$$

for some positive integers C and D.
We may suppose that B is odd, since if B were even, we could set $B = 2B_1$ and have a similar pair of equations.
The first equation in (2.38) is Pythagorean equation, thus surely has solutions. Let,

$$\begin{cases} A = pq, \\ B = p^2 - q^2 \end{cases}$$

so that we get: $C^2 = p^4 - p^2q^2 + q^4$
Thus, (p, q, C) is another solution of given equation.
But, $pq = A = \frac{a}{d_2} \leq a = \frac{x_1y_1}{2b} < \frac{x_1y_1}{2}$, which contradicts minimality of x_1y_1.
Thus, $x_1y_1 = 0$ [minimal non-negative value], yielding the solution, $(0, k, k^2), k \in \mathbb{Z}^+$ and $(k, 0, k^2)$, $k \in \mathbb{Z}^+$.

Case 2: *Both x_1 and y_1 are odd (same parity)*[21]
Then, for some positive integers a and b of different parity (not both odd), with $\gcd(a, b) = 1$, let [Pythagorean Triple]:

$$\begin{cases} x_1^2 - y_1^2 = 2ab \\ x_1y_1 = a^2 - b^2 \\ z_1 = a^2 + b^2 \end{cases}$$

Then:

$$\begin{aligned} \left(x_1^2 + y_1^2\right)^2 &= \left(x_1^2 - y_1^2\right)^2 + \left(2x_1y_1\right)^2 \\ \Rightarrow \left(x_1^2 + y_1^2\right)^2 &= (2ab)^2 + 4\left(a^2 - b^2\right)^2 \\ \Rightarrow \left(x_1^2 + y_1^2\right)^2 &= 4\left(a^4 - a^2b^2 + b^4\right) \\ \Rightarrow \left(\frac{x_1^2 + y_1^2}{2}\right)^2 &= a^4 - a^2b^2 + b^4 \end{aligned}$$

Thus, starting with (x_1, y_1, z_1), we have generated a new solution:

$$\left(a, b, \frac{x_1^2 + y_1^2}{2}\right) = \left(\sqrt{\frac{z_1 + x_1y_1}{2}}, \sqrt{\frac{z_1 - x_1y_1}{2}}, \frac{x_1^2 + y_1^2}{2}\right)$$

But, $z_1^2 = x_1^4 + y_1^4 - x_1^2y_1^2$

$$\left(a, b, \frac{x_1^2 + y_1^2}{2}\right) = \left(\sqrt{\frac{\sqrt{x_1^4 + y_1^4 - x_1^2y_1^2} + x_1y_1}{2}}, \sqrt{\frac{\sqrt{x_1^4 + y_1^4 - x_1^2y_1^2} - x_1y_1}{2}}, \frac{x_1^2 + y_1^2}{2}\right)$$

is a solution to given equation.
We assumed $\gcd(x_1, y_1) = 1$, so, $x_1 \neq y_1 \neq 0$.
Now,a, b must be integers, so firstly, $x_1^4 - x_1^2y_1^2 + y_1^4$ should be a perfect square, its discriminant w.r.t. x_1^2 (and y_1^2) should be zero,

$$\Delta = y_1^2 - 4y_1^2 = 0 \quad \Rightarrow y_1 = 0$$

Contradiction![22] Thus, $x_1 = y_1$ if satisfies the equation is only solution in this case.
Now, for $x_1 = y_1 = k$ we get: $(k, 0, k^2)$ as new, solution. Hence this satisfies the equation, and thus is a solution.
Hence, (k, k, k^2) where, $k \in \mathbb{Z}^+$ is a solution to given equation.

Combining both cases we prove the statement. ☐

---

[21] For both x_1 and y_1 even we first reduce them by cancelling common factors, since, $\gcd(x_1, y_1) = 1.$, and then put them in either case 1 or case 2.

[22] Note that if $\gcd(x_1, y_1) = v > 1$, even then we will arrive at same contradiction, by taking v out of square-root.

2.4.3 Fermat's Last Theorem

Undoubtedly *Fermat's Last Theorem* is one of the most important *Diophantine Equation.* Pierre de Fermat scribbled the following assertion in the margin alongside problem 8 in Book II of the Latin translation, by Bachet, of Diophantus' *Arithmetic* (assertion translated from the Latin as in [16]):

It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general any power higher than the second into powers of like degree. I have discovered a truly remarkable proof which this margin is too small to contain.

This assertion can be restated as:
There exist no non-zero integer solution of $x^n + y^n = z^n$ for $n \geq 3$.

It took hard-work of many brilliant mathematicians over a span of 350 years to prove Fermat's assertion and turn it into a theorem. But when I first saw this theorem, I wondered: *Why can't we apply principle of mathematical induction?.* The following problem was basis of my speculation:

Digression. Prove that for all integers $n \geq 3$, there exist[23] odd positive integers x, y, such that $7x^2+y^2 = 2^n$.

But here instead we need to prove "non-existence" of solutions so we can't use induction. Rather we can try contrapositive of induction, i.e. Method of Finite Descent. But that too fails. Though, Fermat proved his assertion for $n = 4$ by using Method of Infinite Descent! I will now give proof of two special cases and will try to give an outline of proof for general case.

Theorem 2.4.3. *There exist no non-zero integer solution of $x^3 + y^3 = z^3$*

Proof. Assume that the given equation is solvable in non-zero integers[24] and let, (x_1, y_1, z_1) be a non-zero primitive[25] solution with, $x_1y_1z_1 \neq 0$ and $|x_1y_1z_1|$ is minimal.
Now two of the integers x_1, y_1, z_1 must be odd. (standard parity argument). Let, x_1, y_1 be odd numbers. Then:

$$\begin{cases} x_1 + y_1 = 2u \\ x_1 - y_1 = 2v \end{cases}$$

where $u, v \in \mathbb{Z}$. We can assume that $u > 0$, for simplicity.
Solving above set of equations we obtain:

$$\begin{cases} x_1 = u + v \\ y_1 = u - v \end{cases}$$

But since (x_1, y_1, z_1) are solution of given equation we substitute these values in given equation to get:

$$(u + v)^3 + (u - v)^3 = z_1^3$$

$$\Rightarrow 2u(u^2 + 3v^2) = z_1^3 \tag{2.39}$$

Since x_1, y_1 are odd, u, v are of different parity. Thus, $(u^2 + 3v^2)$ is an odd number. Hence,

$$\gcd(2u, u^2 + 3v^2) = \gcd(u, u^2 + 3v^2)$$

Also, $\gcd(x_1, y_1) = 1 \quad \Rightarrow \gcd(u, v) = 1$

$$\Rightarrow \gcd(2u, u^2 + 3v^2) = \gcd(u, 3)$$

Now we will split cases based upon possible values on $\gcd(u, 3)$.

---

[23] Choose: $x_{n+1} = \frac{|x_n - y_n|}{2}$ and $y_{n+1} = \frac{7x_n + y_n}{2}$ and apply weak form of induction. For complete solution refer: pp. 37 of [17]

[24] The proof that I have provided here, uses elementary arithmetic and quadratic reciprocity only. This proof has been taken from [17]. First proof of this theorem was published by Euler, using *Unique Factorization Domain*, but it was complicated, for that proof refer pp.170 of [17]. An elegant proof to this theorem also using *Unique Factorization Domain* was provided by Gauss. For that proof refer pp. 96 of [1] or pp. 441 of [9].

[25] x_1, y_1, z_1 are pairwise prime

Case 1: $\gcd(u, 3) = 1$

Then we write solution of (2.39) in parametric form as:

$$\begin{cases} 2u = t^3 \\ u^2 + 3v^2 = s^3 \\ z_1 = ts \end{cases} \tag{2.40}$$

From this set of equations, we are concerned about second one:

$$u^2 + 3v^2 = s^3$$

Now we will have to analyse this equation in detail in order to deal with given equation.

Proposition 1: *Let n be a positive integer. The equation $u^2 + 3v^2 = n$ is solvable in integers if and only if all prime factors of n of the form $3k - 1$ have even exponents*[26].

Part 1: *A prime p can be written in the form $p = u^2 + 3v^2$ if and only if $p = 3$ or $p = 3k + 1, k \in \mathbb{Z}^+$.*

Indeed, we have $3 = 0^2 + 3(1)^2$. Thus this proves our conjecture for $p = 3$.

Step 1: $p = u^2 + 3v^2 \Rightarrow p$ is a prime of form $3k + 1, k \in \mathbb{Z}^+$

Now, assume $p > 3$ and $p = u^2 + 3v^2$. Then $\gcd(u, p) = 1$ and $\gcd(v, p) = 1$. Therefore, there exists an integer v' such that

$$vv' \equiv 1 \pmod{p} \tag{2.41}$$

Also from our main equation we get:

$$u^2 \equiv -3v^2 \pmod{p}$$

Now using (2.41) it follows that,

$$(uv')^2 \equiv -3 \pmod{p}$$

Thus, -3 is a quadratic residue modulo p. Thus is terms of Legendre symbol:

$$\Rightarrow \left(\frac{-3}{p}\right) = 1$$

Also by Quadratic Residue Multiplication Rule, we get:

$$\Rightarrow \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = 1$$

Further as per Eulers Criterion, we get:

$$\Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$$

From Law of Quadratic Reciprocity:

$$\Rightarrow \left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}\frac{3-1}{2}}$$

Thus we get:

$$\Rightarrow \left(\frac{p}{3}\right) = 1$$

This implies that p is a quadratic residue modulo 3. But only possible quadratic residue[27] for a prime number modulo 3 is 1. Thus:

$$p \equiv 1 \pmod{3}$$

This proves one side implication of our conjecture.

---

[26] Note that prime factors with even powers are always quadratic residue modulo p, for any odd prime number p. Thus we just need to prove that prime factors of n which appear in quadratic residue are of form $3k + 1$.

[27] see Example 1.6.1

Step 2: *p is a prime of the form $3k+1 \Rightarrow p = u^2 + 3v^2$*

Since p is a prime of the form $3k+1$, there exists[28] an integer a such that $a^2 \equiv -3 \pmod{p}$. Clearly $\gcd(a,p) = 1$, and if we set $b = \lfloor \sqrt{p} \rfloor$, then $(b+1)^2 > p$. Thus, there exist $(b+1)^2$ pairs $(c,d) \in \{0,1,\ldots,b\} \times \{0,1,\ldots,b\}$ and $(b+1)^2$ integers of the form $ac+d$ where $c,d \in \{0,1,\ldots,b\}$.
It follows[29] that there exist pairs $(c_1,d_1) \neq (c_2,d_2)$ such that $ac_1+d_1 \equiv ac_2+d_2 \pmod{p}$. Assume $c_1 \geq c_1$ and define

$$\begin{cases} u = c_1 - c_2, \\ v = |d_1 - d_2| \end{cases}$$

Therefore,

$$\begin{cases} 0 < u, v \leq b < \sqrt{p} \\ au + v \equiv 0 \pmod{p} \end{cases}$$

$$\Rightarrow a^2u^2 - v^2 \equiv 0 \pmod{p}$$

Moreover, since $a^2 \equiv -3 \pmod{p}$, we obtain that:

$$p \Big| (a^2+3)u^2 - (3u^2+v^2) \quad \Rightarrow 3u^2 + v^2 = lp$$

where $l \in \mathbb{Z}^+$.
Since we have : $0 < u^2, v^2 < p$, it follows that, $l \in \{1,2,3,\}$
If, $l = 1$ we get: $3u^2 + v^2 = p$, possible.
If, $l = 2$ we get: $3u^2 + v^2 = 2p$, not possible since $2p \equiv 0 \pmod{2} \Rightarrow 3u^2 + v^2 \equiv 0 \pmod{2} \Rightarrow 3u^2 + v^2 \equiv 0 \pmod{4}$, thus p is not odd prime. Contradiction!
If, $l = 3$ we get: $3u^2 + v^2 = 3p$, is possible since we can substitute $v = 3v_1$ to get, $u^2 + 3v_1^2 = p$.
This proves other side of implication.

Part 2: *If $p \geq 3$ is a prime of the form $3k-1$ and $p|u^2+3v^2$, then $p|u$ and $p|v$.*

Let $p \not| u$, we have $\gcd(p,u) = 1$. Therefore, there exists an integer v' such that

$$vv' \equiv 1 \pmod{p} \tag{2.42}$$

Also from our main equation we get:

$$u^2 \equiv -3v^2 \pmod{p}$$

Now using (2.42) it follows that,

$$(uv')^2 \equiv -3 \pmod{p}$$

Thus, -3 is a quadratic residue modulo p. Thus is terms of Legendre symbol:

$$\Rightarrow \left(\frac{-3}{p}\right) = 1$$

leading to (as done in Step 1 of Part 1),

$$\Rightarrow p \equiv 1 \pmod{3}$$

Contradiction!

---

[28] This is superset of case, $p = 12k_1 + 1$, and when $p = 4k_2 + 1$ we can apply Theorem 1.6.3 and 1.6.4 to show *existence* of a, thus -3 is a quadratic residue modulo p.

[29] we used similar argument to prove Theorem 2.2.1

Now we will complete the proof by combining Part 1 and Part 2.
Consider $n = g^2h$, where h is square-free integer. It follows that:

$$h = \prod_{i=1}^{m} p_i$$

where $p_i = 3$ or $p_i \equiv 1 \pmod 3$.[prime numbers]
As proved in Part 1, $p_i = u_i^2 + 3v_i^2$, also since,

$$\big(u_1^2 + 3v_1^2\big)\big(u_2^2 + 3v_2^2\big) = \big(u_1u_2 + 3v_1v_2\big)^2 + 3\big(u_1v_2 - u_2v_1\big)^2$$

Thus we get:

$$h = p_1p_2 \dots p_m = u^2 + 3v^2$$

for some integers u and v.
Finally,

$$n = g^2h = (gu)^2 + 3(gu)^2.$$

Thus proving our proposition.

Proposition 2: *The equation,* $u^2 + 3v^2 = s^3$ *has solution* (u_1, v_1, s_1) *with* s_1 *odd and* $\gcd(u_1, v_1) = 1$ *if and only if there exists integers* α, β *such that :*

$$\begin{cases} u_1 = \alpha\Big(\alpha^2 - 9\beta^2\Big) \\ v_1 = 3\beta\Big(\alpha^2 - \beta^2\Big) \\ s_1 = \alpha^2 + 3\beta^2 \end{cases}$$

where $\alpha \not\equiv \beta \pmod 2$[30] *and* $\gcd(\alpha, 3\beta) = 1$

Step 1: *If there exists integers* α, β *which satisfy given conditions* $\Rightarrow$ (u_1, v_1, s_1) *is a solution of with* s_1 *odd and* $\gcd(u_1, v_1) = 1$

Let (u_1, v_1, s_1) be triples satisfying given conditions in terms of α and β. Verify that:

$$\alpha^2\Big(\alpha^2 - 9\beta^2\Big)^2 + 27\beta^2\Big(\alpha^2 - \beta^2\Big)^2 = \Big(\alpha^2 + 3\beta^2\Big)^3$$

thus (u_1, v_1, s_1) is a solution is a solution of given equation.
Since $\alpha \not\equiv \beta \pmod 2$ we obtain that s_1 is odd.
Now,

$$\gcd(u_1, v_1) = \gcd\Big(\alpha\big(\alpha^2 - 9\beta^2\big), 3\beta\big(\alpha^2 - \beta^2\big)\Big)$$

But, from $\gcd(\alpha, 3\beta) = 1$, it follows that:

$$\gcd\Big(3\beta, \big(\alpha^2 - \beta^2\big)\Big) = \gcd\big(3\beta, \alpha\big) = 1$$

and,

$$\gcd\Big(\alpha, 3\beta\big(\alpha^2 - \beta^2\big)\Big) = \gcd\Big(\alpha, \big(\alpha^2 - \beta^2\big)\Big) = \gcd\big(\alpha, -\beta^2\big) = 1$$

Thus,

$$\Rightarrow \gcd(u_1, v_1) = \gcd\Big(\big(\alpha^2 - 9\beta^2\big), \big(\alpha^2 - \beta^2\big)\Big)$$

$$\Rightarrow \gcd(u_1, v_1) = \gcd\Bigg(\Big(\big(\alpha^2 - 9\beta^2\big) - \big(\alpha^2 - \beta^2\big)\Big), \Big(\alpha^2 - \beta^2\Big)\Bigg) = \gcd\Big(-8\beta^2, \big(\alpha^2 - \beta^2\big)\Big)$$

But, $\alpha \not\equiv \beta \pmod 2$,

$$\Rightarrow \gcd(u_1, v_1) = \gcd\Big(\beta^2, \big(\alpha^2 - \beta^2\big)\Big)$$

$$\Rightarrow \gcd(u_1, v_1) = \gcd\big(\beta^2, \alpha^2\big) = \gcd\big(\beta, \alpha\big) = 1$$

This proves one side of implication.

---

[30] equivalent to saying that both are of different parity

Step 2: (u_1, v_1, s_1) *is a solution with* s_1 *odd and* $\gcd(u_1, v_1) = 1 \Rightarrow$ *there exists integers* α, β *which satisfy given conditions.*

We will prove this by induction over prime factors of s_1.
If $s_1 = 1$, we have $u_1 = \pm 1, v_1 = 0$, and $\alpha = \pm 1, \beta = 0$.
Consider $s_1 > 1$ and let q be a prime divisor of s_1. So

$$s_1 = qr$$

where q and r are odd. We get:

$$s_1^3 = u_1^2 + 3v_1^2 = (qr)^3 \tag{2.43}$$

Now using $\gcd(u_1, v_1) = 1$ and Proposition 1 [since we have showed existence of set of solutions in Step - 1 of this proposition.], for $q = 3k' + 1 = 6k + 1$ (we replace $k' = 2k$, since we have odd primes), there exist integers α_1, β_1 such that:

$$q = \alpha_1^2 + 3\beta_1^2$$

Since q is prime and $q = 6k + 1$, we obtain, $\gcd(\alpha_1, 3\beta_1) = 1$ and $\alpha_1 \not\equiv \beta_1 \pmod 2$.
Further, by parametrization we see that for:

$$\begin{cases} w = \alpha_1(\alpha_1^2 - 9\beta_1^2) \\ f = 3\beta_1(\alpha_1^2 - \beta_1^2) \end{cases}$$

we get:

$$w^2 + 3f^2 = \left(\alpha_1^2 + 3\beta_1^2\right)^3 = q^3 \tag{2.44}$$

From this, by modular arithmetic arguments we get: $w \not\equiv f \pmod 2$ and $\gcd(w, 3f) = 1$.
Now multiply (2.44) and (2.43) to get:

$$q^6 r^3 = \left(u_1^2 + 3v_1^2\right)\left(w^2 + 3f^2\right) = q^3 s_1$$

$$\Rightarrow q^6 r^3 = \left(wu_1 + 3fv_1\right)^2 + 3\left(fu_1 - wv_1\right)^2 = \left(wu_1 - 3fv_1\right)^2 + 3\left(fu_1 + wv_1\right)^2 \tag{2.45}$$

Further:

$$(fu_1 + wv_1)(fu_1 - wv_1) = f^2u_1^2 - w^2v_1^2$$

Using, (2.44)

$$\Rightarrow (fu_1 + wv_1)(fu_1 - wv_1) = f^2u_1^2 - \left(q^3 - 3f^2\right)v_1^2$$
$$\Rightarrow (fu_1 + wv_1)(fu_1 - wv_1) = f^2\left(u_1^2 + 3v_1^2\right) - q^3v_1^2$$

using (2.43)

$$\Rightarrow (fu_1 + wv_1)(fu_1 - wv_1) = f^2s_1^3 - q^3v_1^2 = f^2r^3q^3 - q^3v_1^2$$
$$\Rightarrow (fu_1 + wv_1)(fu_1 - wv_1) = q^3\left(f^2r^3 - v_1^2\right)$$

Therefore:

$$q^3 \Big| (fu_1 + wv_1)(fu_1 - wv_1)$$

But, $\gcd(wfu_1v_1, q) = 1$,

$$q\Big|(fu_1 + wv_1) \quad \text{or} \quad q\Big|(fu_1 - wv_1)$$

Thus both of these can't be satisfied simultaneously.
Therefore, there exists $\lambda \in \{-1, 1\}$ such that:

$$\begin{cases} fu_1 - \lambda wv_1 = q^3\mu \\ wu_1 + 3\lambda fv_1 = q^3\sigma \end{cases}$$

for some integer μ, σ.
Substitute them in (2.45) to get

$$r^3 = \sigma^2 + 3\mu^2$$

Also we can solve above set of equations and use (2.44) to get:

$$\begin{cases} u_1 = \sigma w + 3f\mu \\ v_1 = \dfrac{\sigma f - \mu w}{\lambda} \end{cases}$$

Now, if s_1 has in its decomposition η prime factors, then since $s_1 = qr$, it follows that r has $\eta - 1$ prime factors.
From $\gcd(u_1, v_1) = 1$, we obtain $\gcd(\mu, \sigma) = 1$.
Taking into account that r is odd and that it satisfies the induction hypothesis for $\eta - 1$, we obtain integers α_2, β_2 satisfying the properties (again invoke Proposition 1):

$$\begin{cases} \alpha_2 \not\equiv \beta_2 \pmod 2, \\ \gcd(\alpha_2, 3\beta_2) = 1, \\ \sigma = \alpha_2\left(\alpha_2 - 9\beta_2^2\right) \\ \mu = 3\beta_2\left(\alpha_2^2 - \beta_2^2\right) \\ r = \alpha_2^2 + 3\beta_2^2 \end{cases} \tag{2.46}$$

Thus:

$$s_1 = qr = \left(\alpha_1^2 + 3\beta_1^2\right)\left(\alpha_2^2 + 3\beta_2^2\right)$$

$$\Rightarrow s_1 = \left(\alpha_1\alpha_2 + 3\beta_1\beta_2\right)^2 + 3\left(\alpha_1\beta_2 - \alpha_2\beta_1\right)^2$$

Now, let:

$$\begin{cases} \alpha = \alpha_1\alpha_2 + 3\beta_1\beta_2 \\ \beta = \lambda\left(\alpha_1\beta_2 - \alpha_2\beta_1\right) \end{cases}$$

Thus,

$$\begin{cases} s_1 = \alpha^2 + 3\beta^2 \\ u_1 = \alpha\left(\alpha^2 - 9\beta^2\right) \\ v_1 = 3\beta\left(\alpha^2 - \beta^2\right) \end{cases}$$

Also,

$$\alpha - \beta = (\alpha_1\alpha_2 + \beta_1\beta_2) - (\alpha_1\beta_2 + \beta_1\alpha_2) = (\alpha_1 - \beta_1)(\alpha_2 - \beta_2)$$

$$\Rightarrow \alpha - \beta \equiv (\alpha_1 - \beta_1)(\alpha_2 - \beta_2) \pmod 2$$

But from earlier arguments we know that,$\alpha_1 \not\equiv \beta_1 \pmod 2, \alpha_2 \not\equiv \beta_2 \pmod 2$,

$$\Rightarrow \alpha \not\equiv \beta \pmod 2$$

Also,

$$\gcd(u_1, v_1) = 1 \quad \Rightarrow \gcd(\alpha, 3\beta) = 1$$

Combining Step 1 and Step 2 we prove our Proposition 2.

Now, using Proposition 2 we get:

$$\begin{cases} u = \alpha\left(\alpha^2 - 9\beta^2\right) \\ v = 3\beta\left(\alpha^2 - \beta^2\right) \\ s = \alpha^2 + 3\beta^2 \end{cases}$$

using this in (2.40):

$$2u = t^3 = (2\alpha)(\alpha - 3\beta)(\alpha + 3\beta)$$

Where the factors $2\alpha, \alpha - 3\beta, \alpha + 3\beta$ are pairwise relatively prime, so we can assume:

$$\begin{cases} 2\alpha = Z^3, \\ \alpha - 3\beta = X^3, \\ \alpha + 3\beta = Y^3 \end{cases}$$

Then we obtain, $X^3 + Y^3 = Z^3$ and $|XYZ| \neq 0$, i.e., (X, Y, Z) is a non-zero integral solution to given equation.
Moreover,

$$|XYZ| = t = \sqrt[3]{2u} = \sqrt[3]{x_1 + y_1}$$

But we know that[31]

$$\frac{1}{x_1} + \frac{1}{y_1} < 1 \quad \text{for all positive integers } x_1, y_1 > 2$$

$$\Rightarrow x_1 + y_1 < |x_1 y_1| \quad \text{for all integers } x_1, y_1 \neq 0, 1, 2 \tag{2.47}$$

We can check that for $x_1, y_1 = 1, 2$ we get no value of z_1, so we can safely use above inequality.

$$\Rightarrow |XYZ| < \sqrt[3]{|x_1 y_1|} < |x_1 y_1 z_1|$$

Contradiction to minimality of $|x_1 y_1 z_1|$, thus this case will yield no solution.

Case 2: $\gcd(u, 3) = 3$

Let, $u = 3u_0$ for some integer u_0 and thus (2.39) can be written as:

$$18u_0\left(3u_0^2 + v^2\right) = z_1^3$$

Thus, $18|z_1^3$, z_1 is even thus: $9|z_1^3$, thus, $3|z_1$, we get $z_1 = 3z_0$ for some integer z_0. Thus:

$$2u_0\left(3u_0^2 + v^2\right) = 3z_0^3 \tag{2.48}$$

Now,

$$\gcd(u, v) = 1 \quad \Rightarrow \gcd(v, 3) = 1 \quad \Rightarrow \gcd\left(3u_0^2 + v^2, 3\right) = 1$$

Thus, from (2.48),

$$3\Big|2u_0(3u_0^2 + v^2) \quad \Rightarrow 3\Big|2u_0 \quad \Rightarrow 3\Big|u_0$$

Thus, $u_0 = 3u_e$ for some integer u_e, then:

$$2u_e\left(3u_0^2 + v^2\right) = z_0^3$$

But, $\gcd\left(2u_e, 3u_0^2 + v^2\right) = 1$, we obtain:

$$\begin{cases} 2u_e = \phi^3 \\ 3u_0^2 + v^2 = \psi^3 \\ z_0 = \phi\psi \end{cases} \tag{2.49}$$

where ψ is an odd integer, with $\gcd(v, 3) = 1$.
Again we encounter the similar second equation as in Case-1, so can directly use Proposition - 1 and Proposition - 2 to get:

$$\begin{cases} v = \alpha\left(\alpha^2 - 9\beta^2\right) \\ u_0 = 3\beta\left(\alpha^2 - \beta^2\right) \\ \psi = \alpha^2 + 3\beta^2 \end{cases}$$

---

[31] This is equivalent to: $x_1 + y_1 < x_1 y_1$ or $\frac{y_1}{y_1 - 1} < x_1$

where α, β are integers, $\alpha \not\equiv \beta \pmod 2$ and $\gcd(\alpha, 3\beta) = 1$.
Using, this along with $u_0 = 3u_e$ in (2.49):

$$\phi^3 = 2u_e = \frac{2u_0}{3} = 2\beta\Big(\alpha^2 - \beta^2\Big) = 2\beta(\alpha - \beta)(\alpha + \beta)$$

Now, since $2\beta, (\alpha + \beta), (\alpha - \beta)$ are relatively prime, we get:

$$\begin{cases} \alpha + \beta = Z^3 \\ \alpha - \beta = x^3 \\ 2\beta = Y^3 \end{cases}$$

Since, $X^3 + Y^3 = Z^3$ and $|XYZ| \neq 0$, (X, Y, Z) is a non-zero integer solution of given equation. Moreover:

$$|XYZ| = \phi = \sqrt[3]{2u_e} = \sqrt[3]{\frac{2u_0}{3}} = \sqrt[3]{\frac{2u_1}{9}} < \sqrt[3]{2u}$$
$$\Rightarrow |XYZ| < \sqrt[3]{x_1 + y_1}$$

But, using (2.47), we get:

$$\Rightarrow |XYZ| < \sqrt[3]{|x_1 y_1|}$$
$$\Rightarrow |XYZ| < |x_1 y_1 z_1|$$

Contradicting minimality of $|x_1 y_1 z_1|$. Thus this case also yields no solution.

Combining Case - 1 and Case - 2, we conclude that the given equation has no solution in non-zero integers.

□

Remark: A close relative of above equation: $x^3 + y^3 = z^3 + w^3$ has infinitely many solutions in integers, other than the obvious solutions with $x = z$ or $x = w$ or $x = y$. My favourite example is, Ramanujan-Hardy Number: $1^3 + 12^3 = 9^3 + 10^3 (= 1729)$.

Theorem 2.4.4. *There exist no non-zero integer solution of* $x^4 + y^4 = z^4$

Proof. Let,(x_1, y_1, z_1) be a primitive solution to this equation, such that z_1 is minimal[32]. Now consider following transformation:

$$\begin{cases} x = u, \\ y = v, \\ z^2 = w \end{cases}$$

So, we get an equivalent equation:

$$u^4 + v^4 = w^2 \tag{2.50}$$

with (u_1, v_1, w_1) as a solution and w_1 is minimal. Now substitute:

$$\begin{cases} u_1^2 = a \\ v_1^2 = b, \\ w_1 = c \end{cases}$$

This leads to Pythagorean equation:

$$a^2 + b^2 = c^2$$

We know from Section 2.3.1, that the solutions are:

$$\begin{cases} u_1^2 = a = st, \\ v_1^2 = b = \dfrac{s^2 - t^2}{2}, \\ w_1^2 = c = \dfrac{s^2 + t^2}{2} \end{cases}$$

---

[32] Fermat actually proved a stronger result: *The equation* $x^4 + y^4 = z^2$ *has no solution in non-zero integers.* The argument is similar to the one used here. Then by replacing, $z = t^2$, we get our special case of Fermat's last Theorem as a corollary.

where s, t are relatively prime odd integers. Leading to odd u_1 and even v_1.

Consider: $u_1^2 = st$
Notice that the product, st is odd and equal to a square. But only 0 and 1 are quadratic residue modulo 4. So we must have:

$$st \equiv 1 \pmod 4$$

Thus, both s, t are either both $\equiv 1 \pmod 4$ or both $\equiv 1 \pmod 4$, in any case:

$$s \equiv t \pmod 4 \tag{2.51}$$

Consider: $v_1^2 = \dfrac{s^2 - t^2}{2}$

$$\Rightarrow 2v_1^2 = s^2 - t^2 = (s-t)(s+t)$$

Now, since s and t are odd and relatively prime means that only common factor of $(s-t)$ and $(s+t)$ is 2.

$$\Rightarrow \gcd(s-t, s+t) = 2$$

But from (2.51) we know that, $(s-t)$ is divisible by 4, but then, $(s+t)$ is twice an odd integer. Furthermore we know that $(s-t)(s+t)$ is twice a (even) square. Also, $v_1 = 2v_0$ (even),thus, to satisfy all these conditions:

$$\begin{cases} s - t = 4m^2 \\ s + t = 2n^2 \end{cases}$$

where m, n are integers, n is an odd integer and $2m, n$ are relatively prime.
From this set of equations we can solve for s, t in terms of m, n:

$$\begin{cases} s = n^2 + 2m^2 \\ t = n^2 - 2m^2 \end{cases}$$

Now substitute them back into : $u_1^2 = st$, to get:

$$u_1^2 = n^4 - 4m^4$$

Rearrange terms to get:

$$u_1^2 + 4m^4 = n^4$$

Now, repeat the substitution process:

$$\begin{cases} u_1 = A, \\ 2m^2 = B, \\ n^2 = C \end{cases}$$

Again we get a Pythagorean equation:

$$A^2 + B^2 = C^2$$

Again, we know from Section 2.3.1, that the solutions are:

$$\begin{cases} u_1 = A = ST, \\ 2m^2 = B = \dfrac{S^2 - T^2}{2}, \\ n^2 = C = \dfrac{S^2 + T^2}{2} \end{cases}$$

where S, T are relatively prime odd integers.

Consider: $2m^2 = B = \dfrac{S^2 - T^2}{2}$

$$\Rightarrow 4m^2 = S^2 - T^2 = (S-T)(S+T)$$

Now, since S and T are odd and relatively prime means that only common factor of $(S-T)$ and $(S+T)$ is 2.

$$\Rightarrow \gcd(S-T, S+T) = 2$$

Furthermore we know that $(S-T)(S+T)$ is a perfect square. Thus,

$$\begin{cases} S-T = 2M^2 \\ S+T = 2N^2 \end{cases}$$

where M, N are integers.
From this set of equations we can solve for S, T in terms of M, N:

$$\begin{cases} S = N^2 + M^2 \\ T = N^2 - M^2 \end{cases}$$

Now substitute them into : $n^2 = \dfrac{S^2 + T^2}{2}$, to get:

$$n^2 = M^4 + N^4$$

Thus, (M, N, n) is a solution to our equivalent equation (2.50).But,

$$w_1 = \frac{s^2 + t^2}{2} = \frac{\left(n^2 + 2m^2\right) + \left(n^2 - 2m^2\right)}{2} = n^4 + 4m^2$$

Thus, $w_1 > n$. But this contradicts the minimality of w_1, which further contradicts the minimality of z_1.

Thus, the given equation has no solutions in non-zero integers ☐

Remark: A consequence of this theorem is that the area of a Pythagorean triangle can never be a perfect square.

Theorem 2.4.5. *There exist no non-zero integer solution of $x^n + y^n = z^n$ for $n \geq 3$*

Sketch of Proof. The proof is complicated and is out of scope of this project. Rather I present an outline of proof from [16]:

1. If, $p|n$, say $n = pm$, and if $x^n + y^n = z^n$, then $(x^m)^p + (y^m)^p = (z^m)^p$. Thus if this equation has no solution for prime exponents, then it won't have solution for non-prime exponents either.
2. Let $p \geq 3$ be a prime, and suppose that there is a solution (x_0, y_0, z_0) to $x^p + y^p = z^p$ with x_0, y_0, z_0 non-zero integers and $\gcd(x_0, y_0, z_0) = 1$.
3. Let E_{x_0,y_0} be an elliptic curve, called Frey Curve: $y^2 = x(x + x_0^p)(x - y_0^p)$
4. Wiles's Theorem tells us that E_{x_0,y_0} is modular, that is, its p-defects, a_p follow a Modularity Pattern.
5. Ribet's Theorem tells us that E_{x_0,y_0} is so strange that it cannot possibly be modular.
6. The only way out of this seeming contradiction is the conclusion that the equation $x^p + y^p = z^p$ has no solution in non-zero integers.

Commentary about "Sketch of Proof" of Fermat's Last Theorem

- *How Elliptic Curves and Fermat's Last Theorem got related?*
  In 1983, Gerd Faltings proved a conjecture of Mordell regarding elliptic curves. As a corollary, it stated that curve $X^n + Y^n = 1$ has only finitely many rational points if $n \geq 5$, which meant that there can be only finitely many integer solutions of $x^n + y^n = z^n$ for $n \geq 5$.

- *What is so special about Frey Elliptic Curve?*
  In 1985, Gerhard Frey linked a counter example to Fermat's Last Theorem, if there is one, with an elliptic curve which did not seem to satisfy the Shimura-Taniyama-Weil Conjecture. Frey's idea was: if, for some prime $p > 3$, there are non-zero integers u, v, w such that $u^p + v^p = w^p$, then consider the elliptic curve, now referred as the Frey Curve, $y^2 = x(x + u^p)(x - v^p)$. Thus for first time, Fermat's Last Theorem for any exponent was connected with a cubic curve instead of a higher degree curve which the equation itself defines.

- *What is Shimura-Taniyama-Weil Conjecture ?*
  It states that every elliptic curve is modular. That is, p-defects, a_p's of an elliptic curve exhibit a modularity pattern.

- *What is meant by an elliptic curve being modular?*
  An elliptic curve is called modular if there is a map to it from another special sort of curve called a modular curve.

- *What is meant by p-defects?*
  p-defect, a_p, is defined as difference between the prime number, p, and number of solutions to a given elliptic curve modulo p, N_p.
  $$a_p = p - N_p$$
  The actual mathematical name for the quantity a_p is the *trace of Frobenius.*

- *What does it mean to say that a_p of an elliptic curve exhibit a Modularity Pattern?*
  It means that there is a series:
  $$\Theta = c_1 T + c_2 T^2 + c_3 T^3 + \dots$$
  so that for (most) primes p, the coefficients c_p equals a_p of that elliptic curve.

- *What is Wiles's Theorem?*
  It states that every semistable elliptic curve exhibits a Modularity Pattern.

- *When is an elliptic curve semistable?*
  An elliptic curve is semistable if, for every bad prime $p \geq 3$, the a_p is equal to ± 1.

- *What is meant by bad prime?*
  We say that a prime number, p, is a bad prime, for a given elliptic curve, $y^2 = f(x) = x^3 + ax^2 + bx + c$, if the polynomial $f(x)$ has double or triple root modulo p.

- *What is Ribet's Theorem?*
  It states that for a prime p, if $x^p + y^p = z^p$ with $xyz \neq 0$, then the Frey Curve is not modular.

First General Results on Fermat's Last Theorem : A Historical Account

One of the first general results on Fermat's Last Theorem, as opposed to verification for specific exponents n, was given by *Sophie Germain* in 1823. She proved that if both p and $2p + 1$ are primes then the equation $a^p + b^p = c^p$ has no solutions in integers a, b, c with p not dividing the product abc.

A later result of a similar nature, due to *A. Wieferich* in 1909, is that the same conclusion is true if the quantity $2^p - 2$ is not divisible by p^2 .

In later part of nineteenth century, *Richard Dedekind*, *Leopold Kronecker*, and especially *Ernst Kummer*, developed a new field of mathematics called algebraic number theory and used their theory to prove Fermat's Last Theorem for many exponents, although still only a finite list.

Then, in 1985, *L.M. Adleman*, *D.R. Heath-Brown*, and *E. Fouvry* used a refinement of Germain's criterion together with difficult analytic estimates to prove that there are infinitely many primes p such that $a^p + b^p = c^p$ has no solutions with p not dividing abc.

2.5 Exponential Equations

These are those equations where, the unknowns appear also as exponents. For some refernces on such equations refer pp. 109-111 of [8].

2.5.1 Equations in two unknowns

Theorem 2.5.1. *The equation*

$$x^y = y^x$$

has only one solution in positive integers, with $y > x$. That is $x = 2, y = 4$.

Proof. Suppose that (x_1, y_1), with $y_1 > x_1$ is a solution of given equation. We will follow method of *Parametrization.* Let

$$y_1 = \left(1 + \frac{1}{r}\right) x_1 \quad \text{where, } r = \frac{x_1}{y_1 - x_1} \text{ is a positive rational number}$$

Now substituting this in given equation we get:

$$x_1^{(1+\frac{1}{r})x_1} = y_1^{x_1}$$

$$\Rightarrow x_1^{(1+\frac{1}{r})} = y_1 = \left(1 + \frac{1}{r}\right) x_1 \qquad \Rightarrow x_1^{\frac{1}{r}} = 1 + \frac{1}{r}$$

$$\Rightarrow x_1 = \left(1 + \frac{1}{r}\right)^r$$

Thus we get,

$$y_1 = \left(1 + \frac{1}{r}\right)^{r+1}$$

Let, $r = m/n$, where $\gcd(m, n) = 1$ and $x_1 = t/s$, where $\gcd(t, s) = 1$.
Thus,

$$x_1 = \left(\frac{m+n}{n}\right)^{n/m} = \frac{t}{s} \qquad \Rightarrow \frac{(m+n)^n}{n^n} = \frac{t^m}{s^m}$$

Each side of this equality is an irreducible fraction; also since, $\gcd(m, n) = 1$ we get $\gcd(m + n, n) = 1$, and hence, $\gcd((m + n)^n, n^n) = 1$ and $\gcd(t, s) = 1$ we get $\gcd(t^m, s^m) = 1$. Thus

$$(m+n)^n = t^m \qquad \text{and} \qquad n^n = s^m$$

Thus, there exist natural number k and l such that:

$$\begin{cases} m + n = k^m, & t = k^n \\ n = l^m, & s = l^n \end{cases}$$

$$\Rightarrow m + l^m = k^m$$

$$\Rightarrow k \geq l + 1$$

If, $m > 1$ we would have:

$$k^m \geq (l+1)^m \geq l^m + ml^{m-1} + 1 > l^m + m = k$$

But, this is impossible!
Consequently, if $m = 1$, $r = n/m = n$. This leads to the conclusion that:

$$\begin{cases} x_1 = \left(1 + \frac{1}{n}\right)^n, \\ y_1 = \left(1 + \frac{1}{n}\right)^{n+1} \end{cases} \tag{2.52}$$

where n is a natural number.
Conversely, it is easy to verify that these x_1, y_1 satisfy given equation. Therefore, *all the solutions of equation $x^y = y^x$ in rational numbers x, y with $y > x > 0$ are given by (2.52) where n is a positive integer.*
It follows that $n = 1$ is the only value for which the equation has a solution in positive integers. In this case the solution is $x = 2, y = 4$.

□

Theorem 2.5.2. *The equation*

$$x^y - y^x = 1$$

has precisely two solutions in positive integers. These are $x = 2, y = 1$ *and* $x = 3, y = 2$.

Proof. Suppose that natural numbers x, y satisfy given equation. Then, necessarily, $x^y > 1$, and therefore $x > 1$. If $x = 2$, then as per given equation,

$$2^y = y^2 + 1$$

which implies that y is odd and consequently, $4\big|(y^2 - 1)$. This implies that, $4\big|2^y - 2$ and $2\big|2^{y-1} - 1$. We conclude that $y = 1$.
Also from given equation:

$$x^y > y^x \qquad \Rightarrow \sqrt[x]{x} > \sqrt[y]{y}$$

Further we have:

$$\sqrt[3]{3} > \sqrt[2]{2} = \sqrt[4]{4} > \sqrt[5]{5} > \sqrt[6]{6} > \ldots > \sqrt[1]{1}$$

So, $x = 3, y = 1$ do not satisfy given equation, but $x = 3, y = 2$ do.
Therefore, if x, y is a solution of given equation different from $(2, 1)$ and $(3, 2)$, then either $x = 3, y \geq 4$ or $x \geq 4, y \geq x + 1$. Thus in either case we have $y \geq x + 1$.
Let $y - x = a \in \mathbb{Z}^+$, then

$$\frac{x^y}{y^x} = \frac{x^{x+a}}{(x+a)^x} = \frac{x^a}{\left(1 + \frac{a}{x}\right)^x} \tag{2.53}$$

But, as we know, for *base of natural logarithm*,$e^t > 1 + t$ whenever $t > 0$, this implies that for $t = a/x$ we have

$$\left(1 + \frac{a}{x}\right)^x < e^a$$

using this in (2.53) and by $x \geq 3 > e$, we obtain:

$$\frac{x^y}{y^x} > \frac{x^a}{e^a} = \left(\frac{x}{e}\right)^a \geq \frac{x}{e} \geq \frac{3}{e} > 1.1$$

Hence,

$$x^y - y^x > \frac{y^x}{10} \geq \frac{4^3}{10} > 1$$

contradicting our assumption that (x, y) is solution of given equation. This leads us to the conclusion that the given equation has no solution different from $x = 2, y = 1$ and $x = 3, y = 2$. □

2.5.2 Equations in three unknowns

Theorem 2.5.3. *The equation*

$$x^x y^y = z^z$$

has infinitely many solutions in positive integers, different from 1.

Proof. A parametric solution to this equation was found by Chao Ko[33] and is given by:

$$\begin{cases} x = \left(2^{\left((2^n - n - 1)2^{n+1}\right) + 2n}\right)\left((2^n - 1)^{2(2^n - 1)}\right) \\ \\ y = \left(2^{(2^n - n - 1)2^{n+1}}\right)\left((2^n - 1)^{2(2^n - 1) + 2}\right) \\ \\ z = \left(2^{\left((2^n - n - 1)2^{n+1}\right) + (n+1)}\right)\left((2^n - 1)^{2(2^n - 1) + 1}\right) \end{cases}$$

for any positive integer n. □

---

[33] *"Note on the Diophantine equation $x^x y^y = z^z$", J. Chinese Math. Soc., Vol 2, pp. 205-207 (1940)*

Conclusion

I have discussed about 40 theorems and 25 examples related to “Diophantine Equations” in this project report.

Among the 23 problems posed by David Hilbert in the lecture delivered before the International Congress of Mathematicians at Paris in 1900, tenth problem is regarding Diophantine equation, it states:

Given a Diophantine equation with any number of unknown quantities and with integral numerical coefficients. To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.

This problem was solved in 1970 by Yuri Matiyasevich, following works of Martin Davis, Hilary Putnam and Julia Robinson. The solution is negative, there is no hope of producing a complete theory of the subject. But still, Michel Waldschmidt, in his paper “Open Diophantine Problems” (Moscow Mathematical Journal, Vol. 4, No. 1, January-March 2004, pp. 245-305) states that there is still a hope for a positive answer to Hilbert’s Tenth Problem, if one restricts original problem to a limited number of variables, say $n = 2$.

I would like to finish my project report with following comments:

- Little is known about the unique factorization property of $\mathbb{Q}[\sqrt{d}]$ for $d > 0$. What we know is that $\mathbb{Q}[\sqrt{d}]$ is a Unique Factorization Domain (i.e. the ring of algebraic integers of $\mathbb{Q}[\sqrt{d}]$ is a Unique Factorization Domain) for $d = 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 33, 37, 41, 53, 57, 61, 69, 73, 77, 89, 93, 97$.
- Among the two problems considered, i.e., computing the number solutions and generating the solutions, the first one is by far the most complex.
- If we are given a rational point on cubic curve we can find other solutions, but there is no known method to determine in a finite number of steps whether any given rational cubic has rational point.
- *Exponential Diophantine Equations* constitute some very interesting conjectures, for example, following conjecture was made by Siva Shankaranarayana Pillai at a conference of Indian Mathematical Society in Aligarh (1945) :

  Let k be a positive integer. The equation

  $$x^p - y^q = k$$

  where the unknowns $x, y, p, q \geq 2$ take integer values, has only finitely many solutions (x, y, p, q).

Bibliography

[1] Heinrich Dörrie : *100 Great Problems of Elementary Mathematics - Their History and Solution*, Dover Publications Inc. (1965)

[2] C. Stanley Ogilvy & John T. Anderson : *Excursions in number theory*, Oxford University Press Inc. (1966)

[3] H. M. Stark : *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. Vol. 14 (1), pp. 1-27, doi:10.1307/mmj/1028999653 (1967)

[4] D. T. Walker : *On the diophantine equation* $mX^2 - nY^2 = \pm 1$, American Mathematical Monthly, Vol. 74 (5), pp. 504-513, doi:10.2307/2314877 (1967)

[5] Louis J. Mordell : *Diophantine Equations*, Academic Press Inc (1969)

[6] I. N. Herstein : *Topics in Algebra*, John Wiley & Sons, Xerox Corporation (1975)

[7] A. O. Gelfond : *Solving Equations in Integers*, English translation, Little Mathematics Library, Mir Publishers Moscow (1981)

[8] W. Sierpińksi : *Elementary Theory of Numbers*, PWN-Polish Scientific Publishers, ISBN 0-444-86662-0 (1988)

[9] Ivan Niven, Herbert S. Zuckerman & Hugh L. Montgomery : *An Introduction to the Theory of Numbers*, Fifth Edition, John Wiley & Sons Inc, ISBN 0-417-62546-9 (1991)

[10] Joseph H. Silverman & John Tate : *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, Springer-Verlag New York, ISBN 3-540-97825-9 (1992)

[11] C. S. Yogananda : *Fermat's Last Theorem - A Theorem at Last!*, Resonance, Indian Academy of Sciences, Vol. 1, No. 1, pp. 71-79 (1996)

[12] R. A. Mollin, K. Cheng & B. Goddard : *The diophantine equation* $Ax^2-By^2 = C$ *solved via continued fraction*, Acta Math. Univ. Comenianae, Vol. LXXI (2), pp. 121-138 (2002)

[13] Dinesh Khurana : *On GCD and LCM in Domains - A Conjecture of Gauss*, Resonance, Indian Academy of Sciences, Vol. 8, No. 6, pp. 72-79 (2003)

[14] M. Ya. Antimirov & A. Matvejevs : *Evaluation of the Number of Non-Negative Solutions of Diophantine Equations*, 5th Latvian Mathematical Conference, Daugavpils, Latvia (2004)

[15] H. Davenport : *The Higher Arithmetic*, Eighth Edition, Cambridge University Press, ISBN 978-0-511-45555-1 eBook(EBL) (2008)

[16] Joseph H. Silverman : *A Friendly Introduction to Number Theory*, Indian Edition, Pearson Education Inc, ISBN 978-81-317-2851-2 (2009)

[17] Titu Andreescu, Dorin Andrica & Ion Cucurezeanu : *An Introduction to Diophantine Equations - A Problem Based Approach*, Birkhäuser, Springer Science+Business Media, ISBN 978-0-8176-4548-9 (2010)

[18] D.M. Smirnov : *Algebraic System*, Encyclopedia of Mathematics, Retrieved from "http://www.encyclopediaofmath.org/index.php?title=Algebraic_system&oldid=12791"

Prepared in $\LaTeX\,2_\varepsilon$ by Gaurish Korpal