Diophantine Tuples

Ganesh Sankar

July 26, 2022

1 Introduction

The Greek Mathematician Diophantus of Alexandria first studied the problem of finding four numbers that satisfied the following property: one plus the product any two elements in the set is a perfect square. He found the following set of four rational numbers that satisfy this condition: {1/16, 33/16, 17/4, 105/16}.

Later, Fermat found the first set of four integers to satisfy the condition, the set {1, 3, 8, 120}. Euler was able to add the rational number 777480 / 8288641 to the set such that this property was preserved. This problem has a long history, attracting the attention of many,including Fermat, Baker, Davenport etc, with significant progress made in recent times due to Dujella (2001a) Dujella (2001b) and Dujella (1998).

Definition 1. A set of m numbers $(a_1,\ a_2, ...,\ a_m)$ is called a Diophantine *m-tuple* if $\mathrm{a}_i \cdot a_j + 1$ is a perfect square for all $1 \leq i < j \leq m$.

Definition 2. A set of m numbers $(a_1,\ a_2, ...,\ a_m)$ is called a D(n) *m-tuple* if $\mathrm{a}_i \cdot a_j + n$ is a perfect square for all $1 \leq i < j \leq m$.

These sets have been explored across many different fields such as integers, rational numbers, Quadratic fields, Gaussian integers, and have many problems and concepts related to them.
In this paper we explore the extensions of Diophantine tuples.

2 Elliptic Curves

2.1 Background

We discuss the applications of elliptic curves to diophantine tuples. Elliptic curves have a wide variety of use in mathematics, as they can be applied to many different problems from cryptography and algebraic number theory to complex analysis. These figures can be described by the following equation:

$$y^2 = ax^3 + bx^2 + cx + d.$$

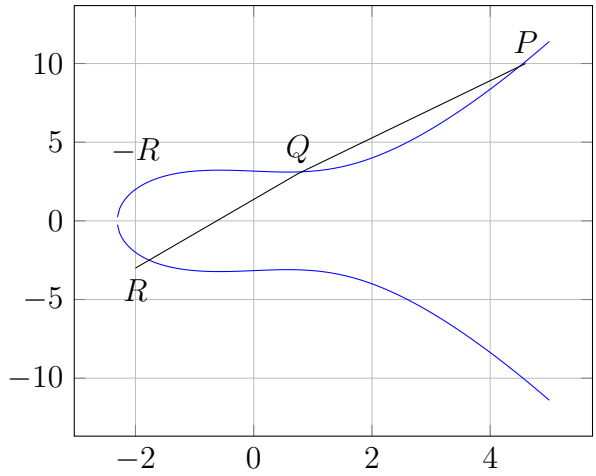

Figure 1.

The set of rational numbers on the curve can be described as the group $E(\mathbb{Q})$ with the group operation addition. Let P and Q be two distinct points on $E(\mathbb{Q})$. In the context of elliptic curves, $P+Q$ is defined as the reflection of $P*Q$ over the $x-axis$, where $P*Q$ is the intersection point of the line PQ with the curve other than P or Q. $P+P=2P$ is defined similarly, but P*P is the intersection point of the tangent line at P with the curve other than P. However, for $E(\mathbb{Q})$ to be a group, there must be an identity element; since there is no point in the plane that works, we can create an extra point O "at infinity." O must be a point on every vertical line for it to serve as the identity element. $P+O=P$ and $O+P=P$ for all P, so our new set satisfies all the conditions to be a group.

Theorem 1 (Poincaré) [Silverman] Let K be a field and let E be an elliptic curve that is given by the equation of the form

$$y^2 = x^3 + Ax + b, A, B \in K$$

Let $E(K)$ denote the points of E with coordinates in K,

$$E(K) = \{(x,y) \in E : x, y \in K\} \cup \{O\}$$

then $E(K)$ is a subgroup of the group of all points on E.

Thus the set $E(\mathbb{Q}) = \{(x,y) : y^2 = x^3+ax^2+bx+c : x, y \text{ rational}\} \cup \{\text{O}\}$ is a subgroup of all the points on E.

2.2 Extending Diophantine Tuples in Rational numbers

Let $\{a,b,c\}$ be a diophantine triple, which satisfies $ab+1=r^2$, $bc+1=s^2$, and $ac+1=t^2$. To extend this set (add another element, x), $ax+1$, $bx+1$, $cx+1$ must all be in Q^{*2}. Multiplying these conditions, we get that

$$y^2 = (ax+1)(bx+1)(cx+1) \tag{1}$$

However, not only does this equation need to be satisfied for rational numbers x and y for the tuple to be extended, the original condition of each of $ax+1$, $bx+1$, and $cx+1$ each being perfect squares must be satisfied.

First, let's analyze the elliptic curve, $y^2 = (ax + 1)(bx + 1)(cx + 1)$. With the transformations

$$x \to x/abc, y \to y/abc \tag{2}$$

we get the new equation

$$y^2 = (x + bc)(x + ac)(x + ab) \tag{3}$$

Let $E(\mathbb{Q})$ the set of points with rational coordinates on equation (1), and $E'(\mathbb{Q})$ be that of the transformed curve. Some notable points on $E(\mathbb{Q})$ are

$$A = (-1/a, 0), B = (-1/b, 0), C = (-1/c, 0) \tag{4}$$

and

$$P = (0, 1), S = (1/abc, rst/abc). \tag{5}$$

$E'(\mathbb{Q})$ contains the points

$$A = (-bc, 0), B = (-ac, 0), C = (-ab, 0)$$

$$P' = (0, abc), S' = (1, rst)$$

This is just to convert the elliptic curve with constant term 1, in order to make our calculations easier. At any point we can use whichever one that is easier to work with. Let us shift back to $E(\mathbb{Q})$.

$2E(\mathbb{Q})$ is the set of all points with rational coordinates on the curve which can be expressed as 2P for some point P in $E(\mathbb{Q})$.
In fact, $S \in 2E(\mathbb{Q})$. $S = 2R, where$

$$R = (\frac{rs + rt + st + 1}{abc}, \frac{(r + s)(r + t)(s + t)}{abc}) \tag{6}$$

Theorem 2. The x-coordinate of the point T $\in E(Q)$ satisfies (3) *iff* T - P $\in 2E(Q)$.
Proof. The proof can be done by 2 descent proposition for elliptic curves, as done in Dujella (2001a) [Proposition 1].

Thus, we can add $x(T)$, (the x coordinate of T), to the existing diophantine triple to get $\{a, b, c, x(T)\}$, which is a diophantine quadruple. We also get that every diophantine triple can be extended to a diophantine quadruple using this construction.

Theorem 3. If T satisfies Theorem 1, then for the points $T \pm S$ it holds that $x(T)x(T \pm S) + 1$ is a square.
Proof. The proof of this theorem can be achieved by direct computation.

Lemma 1. The numbers $T \pm S$ satisfy Theorem 1.
Proof. This statement can be proved due to the fact that $S \in$2E(Q).

We get that the diophantine quadruple $\{a, b, c, x(T)\}$ can always be extended to a diophantine quintuple $\{a, b, c, x(T), x(\text{T+S})\}$ or $\{a, b, c, x(T), x(\text{T-S})\}$.

So far, we can conclude that there are infinitely many diophantine triples, quadruples, and quintuples, given in the previous form.

Adding *both* $x(T+S)$ and $x(T-S)$ to $\{a, b, c, x(T)\}$, we get a set of six numbers which is almost a diophantine sextuple; however one condition is not met: $x(T+S)x(T-S)+1$ must be a perfect square. This condition is met if S is a point of order 3. Thus, since there are infinitely many points of order 3, there can be infinitely many constructions of diophantine sextuples.

3 Diophantine Tuples in integers

We now explore diophantine tuples throughout the integers.

Definition 1. A set of m positive integers

$$(a_1,\ a_2, ...,\ a_m)$$

is called a Diophantine m-tuple if

$$a_i\ a_j + 1$$

is a perfect square for all

$$1 \leq i < j \leq m$$

We can use what we have came up with on diophantine tuples in rational numbers, since all integers are rational numbers. First we can look at some diophantine integer tuples for smaller values of m.

Some examples for diophantine triples are sets of the form:

$$\{k-1, k+1, 4k\} \text{ or } \{F_{2k}, F_{2k+2}, F_{2k+4}\}$$

Since $S \in E(Q)$, by Theorem 1, either $x(P+S)$ or $x(P-S)$ can be added to the original diophantine triple, $\{d, e, f\}$

Let $y = mx + b$ be the equation of the line between P' and S', and x' be the x coordinate of $P' + S'$

$$(mx+b)^2 = x^3 + ax^2 + bx + c = (x+de)(x+df)(x+ef)$$

$$x^3 + (a-m^2)x^2 + (b-2mb)x + (c-b^2) = 0$$

The slope between P' and S' is $rst - def$, which is m. So:

$$x' = m^2 - a - (0+1) = (rst-def)^2 - (de+df+ef) - 1$$

$$x' = (de+1)(df+1)(ef+1) - 2rstdef + (def)^2 - (de+df+ef) - 1 =$$
$$2(def)^2 + def(d+e+f) - 2rstdef$$

Therefore, the x coordinate of $P+S$ is equal to $d+e+f+2def-2rst$.
Similarly, the coordinate of $P-S$ is equal to $d+e+f+2def+2rst$, so we can extend any diophantine triple in integers to a diophantine quadruple.

4 Solutions by Pellian equations

Suppose the set (a, b, c) is a diophantine triple, and let $ab+1 = x^2$, $bc+1 = y^2$, $ac+1 = z^2$ for integers x, y, z. We get the following system of two Pellian equations:

$$bz^2 - cy^2 = b - c \tag{7}$$

$$az^2 - cx^2 = a - c \tag{8}$$

We are tasked with finding integer solutions (x, y, z) to (8). These equations have solutions that are of exponential and recursive sequences, leading us to the problem of finding their intersection. This system can be completely solved for specific (a, b, c).

Now let us consider these equations with no restrictions.

Lemma 1. If there are integers (z, x) and (z, y) that satisfy (8), theory of Pellian equations says that there exist finite sets $i \in \{1, .., i_0\}$ and $j \in \{1, .., j_0\}$ such that

$$z\sqrt{a} + x\sqrt{c} = (z_0^{(i)}\sqrt{a} + x_0^{(i)}\sqrt{c})(s + \sqrt{ac})^m \tag{9}$$

$$z\sqrt{b} + y\sqrt{c} = (z_1^{(j)}\sqrt{b} + y_1^{(j)}\sqrt{c})(t + \sqrt{bc})^m \tag{10}$$

where $(z_0^{(i)}, x_0^{(i)})$ and $(z_1^{(j)}, y_1^{(j)})$ are any pairs of base solutions that can be used to generate the solutions (z, x) and (z, y). Given that $(z_0^{(i)}, x_0^{(i)})$ and $(z_1^{(j)}, y_1^{(j)})$ are solutions, it can be proved using induction that (z, x) and (z, y) are solutions.

Another way to find solutions of diophantine tuples is by solving these simultaneous Pell's equations. Integer solutions for (z, x) and (z, y) can be expressed recursively, and the intersection of solutions for z can produce solutions to the system of equations, and therefore to the extension of diophantine tuples. We can obtain lower and upper bounds for these solutions by using minimality, linear forms and modular congruences. This method was used to prove the bound on the size of diophantine tuples.

References

A. Dujella. Complete solution of a family of simultaneous pellian equations. *Acta Math. Inform. Univ. Ostraviensis*, 6:59–67, 1998. URL https://www.sciencedirect.com/science/article/pii/S0022314X00926271.

A. Dujella. Diophantine m-tuples and elliptic curves. *Journal de Theorie des Nombres*, 13(10):111–124, 2001a. URL https://www.jstor.org/stable/43972600.

A. Dujella. An absolute bound for the size of diophantine m-tuples. *Journal of Number Theory*, 89:126–159, 2001b. URL https://web.math.pmf.unizg.hr/~duje/pdf/bound.pdf.

J. H. Silverman. An introduction to the theory of elliptic curves. *Brown University and NTRU Cryptosystems, Inc.* URL https://www.math.brown.edu/johsilve/Presentations/WyomingEllipticCurve.pdf.