Diophantine Tuples

Ganesh Sankar

Euler Math Circle

July 6, 2022

Introduction

Definition.

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

- These sets have been studied in many different fields; such as $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{Z}[\mathrm{i}]$, $\mathbb{Z}[\sqrt{d}]$, $\mathbb{Z}[X]$, and others.
- 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 and others.

Examples

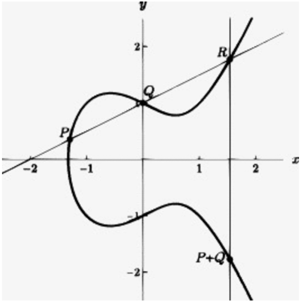
- $(\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16})$ in rational numbers
- (1, 3, 8, 120) in integers
- 777480/8288641
- $(F_k, F_{k+2}, F_{k+4}, 4F_{2k+1}F_{2k+2}F_{2k+3})$
- $(x-1, x+1, 4x)$

Regular Diophantine quadruple: $(a,b,c) => (a,b,c,d)$

$$d = a+b+c+2abc \pm 2rst$$

where $ab+1 = r^2$, $bc+1 = s^2$, $ac+1 = t^2$

Elliptic Curves



The set of rational numbers on an elliptic curve E can be described as the subgroup $E(\mathbb{Q})$ with the group operation addition.
$E(\mathbb{Q}) = \{(\text{x, y}) : y^2 = ax^3 + bx^2 + cx + d : x, y \text{ rational}\} \cup \{O\}$

Elliptic Curves (cont.)

The Elliptic Curve group

1. O is the identity element
2. Let $P, Q \in E(\mathbb{Q})$ for $P \neq Q$
3. Define the intersection of the line through P and Q with E as $P * Q$
4. $P + Q$ is defined as the reflection of $P * Q$ over the $x - axis$
5. $P + P = 2P$ is defined the same way, but $P * P$ is the intersection of the line tangent to E at P with E
6. A point has order n if $nP = O$, $P \neq O$
7. The number of independent basis points with infinite order is the rank of the curve.

Relations to Diophantine Tuples

Let (a, b, c) be a diophantine triple with $ab + 1 = r^2$, $bc + 1 = s^2$, $ac + 1 = t^2$.
For us to extend this set to (a, b, c, x), $ax + 1$, $bx + 1$, and $cx + 1$ must all be perfect squares. Multiplying these conditions,

$$y^2 = (ax + 1)(bx + 1)(cx + 1)$$

Define

$$P = (0, 1), S = (\frac{1}{abc}, \frac{rst}{abc})$$

Extensions of Diophantine Tuples

Theorem.

The $x-coordinate$ of the point $T \in E(Q)$ forms the diophantine quadruple $(a, b, c, x(T))$ *iff* T-P $\in 2E(Q)$.

It can be verified that $S \in 2E(\mathbb{Q})$. By the above, the original diophantine triple (a, b, c) can be extended with $x(P \pm S)$. In fact,

$$x(P \pm S) = a + b + c + 2abc \pm 2rst$$

Extensions of Diophantine Tuples

$x(T \pm S)$ can be extended to the existing diophantine quadruple, to create a rational diophantine quintuple $(a, b, c, x(T), x(T \pm S))$

$x(T)x(T \pm S) + 1$ is always a perfect square and if T satisfies $T - P$ $\in 2E(\mathbb{Q})$,T$\pm S$ also does.

$(a, b, c, x(T), x(T + S), x(T - S))$ is a diophantine sextuple, if $x(T + S)x(T - S) + 1$ is a perfect square

There are infinitely many diophantine sextuples. It can be shown that $x(T + S)x(T - S) + 1$ is a perfect square if S is a point of order 3, which is satisfied if: $x(2S) = x(-S)$

Integer points on the Elliptic Curve

We have always the following "integer points:

$$(0, \pm 1), (d_-, \pm(at + rs)(bs + rt)(cr + st)), (d_+, \pm(at - rs)(bs - rt)(cr - st))$$

and (-1,0) if a, b, or c is 1.
The question is if these are the only integer points on the curve E. For some families of Diophantine triples it is possible to prove that there are no other integer points on E given their rank.
There are 207 quadruples with $max(a, b, c, d) < 10^6$, and each one is regular.

Theorem.

There does not exist a diophantine quintuple in integers.

In Gaussian Integers

Gaussian Integers: Numbers of the form $a + bi$, where $a, b \in \mathbb{Z}$
A set of nonzero Gaussian integers $(a_1, a_2, ..., a_m) \subset Z[i]$ is said to have the property $D(z)$ if the product of any two distinct elements increased by z is a square of a Gaussian integer.

Theorem.

If $z = a + bi$ is not representable as a difference of the squares of two Gaussian integers, there does not exist a diophantine quadruple with the property $D(z)$

Further Questions

1. $D(n)$ tuples
2. Quadratic Fields

Thank you for Listening!