Generalised Diophantine $m$-tuples

Anup B. Dixit

Chennai Mathematical Institute

Fields Number Theory Seminar
November 16, 2020
Definition

A set of $m$ positive integers $\{a_1, a_2, \cdots, a_m\}$ is called a **Diophantine $m$-tuple** if $a_i a_j + 1$ is a perfect square for all $1 \leq i < j \leq m$.

**Fermat:** $\{1, 3, 8, 120\}$

**Euler:** $\{a, b, a + b + 2r, 4(r + a)(r + b)\}$, where $ab + 1 = r^2$

If $a = 1, b = 3$, we get the Fermat’s quadruple.

**Baker and Davenport:** If $\{1, 3, 8, d\}$ is a Diophantine quadruple, then $d = 120$.

**Question**

*Are are any Diophantine quintuples/sextuples/septuples? Can there be an infinite Diophantine tuple?*
Siegel’s theorem

Let \( S = \{a_1, a_2, a_3, \ldots \} \) be a Diophantine tuple. Consider the elliptic curve
\[
y^2 = (a_1x + 1)(a_2x + 1)(a_3x + 1).
\]

Then, \( x = a_4, a_5, \ldots \) each generate an integer point on this curve.

Theorem (Siegel)

The number of integer points on the elliptic curve \( y^2 = x^3 + ax + b \) is finite.

Thus,
\[
|S| < \infty.
\]

Dujella (2001-2004): There are no Diophantine sextuples and at most finitely many Diophantine quintuples.

Togbé-Ziegler (2019): There are no Diophantine quintuples.

Question

If \( \{a, b, c, d_1\} \) and \( \{a, b, c, d_2\} \) are Diophantine quadruples, is \( d_1 = d_2 \)? (Unknown!)
Property $D(n)$

Definition
A set of $m$ positive integers $\{a_1, a_2, \cdots, a_m\}$ is called a Diophantine $m$-tuple with property $D(n)$ if $a_ia_j + n$ is a perfect square for all $1 \leq i < j \leq m$.

Quintuple: $\{1, 33, 105, 320, 18240\}$ has property $D(256)$.

Question
Let $S = \{a_1, a_2, \cdots, a_m\}$ be a Diophantine $m$-tuple with property $D(n)$. Can $m$ be arbitrarily large?

Applying Siegel’s theorem to the elliptic curve

$$y^2 = (a_1x + n)(a_2x + n)(a_3x + n),$$

we conclude that $m < \infty$. 
Caporaso-Harris-Mazur conjecture

Conjecture (Caporaso-Harris-Mazur)

Given any curve $C/\mathbb{Q}$ of genus $g \geq 2$, there exists $\kappa(g)$, independent of the curve, such that $|C(\mathbb{Q})| < \kappa(g)$.

Let $S = \{a_1, a_2, \ldots, a_m\}$ has property $D(n)$. Consider the curve

$$y^2 = (a_1x + n)(a_2x + n) \cdots (a_5x + n).$$

By CHM-conjecture, there $m$ is bounded (with the bounds independent of $a_i$'s and $n$).

Definition

For $n \in \mathbb{N}$, define

- $M(n) := \sup\{|S| : S$ is a Diophantine tuple with property $D(n)\}$.
- $A(n) := \sup\{|S \cap [n^3, \infty)| : S$ is a Diophantine tuple with property $D(n)\}$. 
Bounds on $M(n)$

- CHM conjecture $\implies M(n) = O(1)$.
- (Dujella): $A(n) \leq 24$ and $M(n) = O(\log n)$.
- (Güloğlu, Ram Murty): Under the Paley graph conjecture, for every $\epsilon > 0$
  $$M(n) = O_\epsilon(\log n)^\epsilon.$$
Generalised Diophantine $m$-tuples

Definition

A set of $m$ positive integers $S = \{a_1, a_2, \ldots, a_m\}$ is said to satisfy property $D_k(n)$ if $a_i a_j + n$ is a $k$-th power for $1 \leq i < j \leq m$.

For $n \in \mathbb{N}$, define

- $M_k(n) := \sup\{|S| : S \text{ has property } D_k(n)\}$.
- $M_k(n; L) := \sup\{|S \cap [n^L, \infty)| : S \text{ has property } D_k(n)\}$.

Considering the curve

$$y^k = (a_1 x + n)(a_2 x + n) \cdots (a_5 x + n),$$

CHM conjecture $\implies M_k(n)$ and $M_k(n; L)$ are finite and independent of $n$. 
The $n = 1$ case

Theorem (Bugeaud, Dujella)

- $M_3(1) \leq 7$, $M_4(1) \leq 5$,
- $M_k(1) \leq 4$ for $5 \leq k \leq 176$,
- $M_k(1) \leq 3$ for $k \geq 177$. 
Main theorem

Theorem (A. Dixit, S. Kim, M. R. Murty)

For $k \geq 3$,

(a) For $L > 1$,

$$M_k(n, L) \ll_k 1,$$

where the implied constant is independent of $n$. In fact, $M_k(n, L) \ll \log k$.

(b) Unconditionally,

$$M_k(n) \ll_k \log n.$$

(c) Assuming the Paley graph conjecture, for any $\epsilon > 0$,

$$M_k(n) \ll_{k, \epsilon} (\log n)^\epsilon.$$
The Gallagher’s Large Sieve

**Question**

Given a set $S \subset [1, N]$. Define $S_p = S \pmod{p}$ for a prime $p$. Suppose we knew $|S_p|$ for many primes $p$. Can we say how large $|S|$ is?

Write $S(p, a) := \{s \in S : s \equiv a \pmod{p}\}$. Then,

$$|S| = \sum_{a \pmod{p}} |S(p, a)|.$$

By Cauchy-Schwarz inequality,

$$\frac{|S|^2}{|S_p|} \leq \sum_{a \pmod{p}} |S(p, a)|^2.$$

Hence,

$$|S|^2 \sum_{p \in P} \frac{\Lambda(p)}{|S_p|} \leq \sum_{p \in P} \Lambda(p) \sum_{a \pmod{p}} |S(p, a)|^2 \leq \sum_{p \in P} \Lambda(p) \sum_{s, t \in S} 1$$

$$\leq \sum_{s, t \in S} \sum_{p \in P, p|(s-t)} \Lambda(p) \leq |S| \sum_{p \in P} \Lambda(p) + (\log N)|S|(|S| - 1).$$
The Gallagher’s Sieve

**Theorem**

Let $S$ be a subset of $\{1, 2, \ldots, N\}$ for some positive integer $N$. For any $1 < Q \leq N$, we have

$$|S| \leq \frac{\sum_{p \leq Q} \log p - \log N}{\sum_{p \leq Q} \frac{\log p}{|S_p|} - \log N},$$

where $S_p = S \pmod{p}$, provided the denominator is positive.
Idea of proof for $k = 2$

Let $S = \{a_1, a_2, \cdots, a_m\}$ be a Diophantine $m$-tuple with property $D(n)$.

For $i = 1, -1$, let

$$S_i := \left\{ a \in S_p : \left( \frac{a}{p} \right) = i \right\}.$$ 

Then,

$$|S_p| \leq |S_1| + |S_{-1}| + 1.$$ 

Observe

$$|S_i|(|S_i| - 1) = \sum'_{a,b \in S_i} \left( \frac{ab + n}{p} \right).$$
Vinogradov's inequality

Theorem (Vinogradov)

Let $\chi \pmod{q}$ be a non-trivial Dirichlet character and $n$ be an integer such that $(n, q) = 1$. If $A \subseteq \mathbb{Z}/q\mathbb{Z}^*$ and $B \subseteq \mathbb{Z}/q\mathbb{Z}^* \cup \{0\}$, then

$$\sum_{a \in A} \sum_{b \in B} \chi(ab + n) \leq \sqrt{2q|A||B|}.$$ 

Setting $A = B = S_i$, we deduce

$$|S_i|(|S_i| - 1) = \sum_{a,b \in S_i} \left( \frac{ab + n}{p} \right) \ll |S_i|\sqrt{p}.$$ 

Thus, $|S_p| \ll \sqrt{p}$. Choosing $N = n^3$ and $Q = (\log N)^2$ and applying Gallagher’s Sieve, get

$$|S| \ll \log n.$$
Paley Graph Conjecture

Conjecture (Paley)

Let $\epsilon > 0$ be a real number, $A, B \subseteq \mathbb{F}_p$ for an odd prime $p$ with $|A|, |B| > p^\epsilon$, and $\chi$ be any non-trivial multiplicative character modulo $p$. Then, there is some number $\delta > 0$ such that

$$\left| \sum_{a \in A, b \in B} \chi(a + b) \right| \leq p^{-\delta} |A| |B|.$$

Thus,

$$|S_i|(|S_i| - 3) \leq \sum_{a, b \in S_i} \left( \frac{ab + n}{p} \right) = \left| \sum_{a, b \in S_i} \left( \frac{b + na^{-1}}{p} \right) \right| \leq p^{-\delta} |S_i|^2$$

by setting $A = S_i$ and $B = nS_i^{-1}$ under Paley graph. One immediately gets $|S_p| \ll p^\epsilon$ and applying Gallagher’s Sieve,

$$|S| \ll_\epsilon (\log n)^\epsilon.$$
For $k \geq 3$

Let $S := \{a_1, a_2, \cdots, a_m\}$ be a Diophantine $m$-tuple with property $D_k(n)$.
If each $|a_i| \leq n^L$ for some $L > 1$, then adaptation of previous methods gives

$$m \ll \log n$$

and under the Paley-graph conjecture

$$m \ll_{\epsilon} (\log n)^{\epsilon}.$$

Key step: To show that $M_k(n; L) \ll_k 1$. 
Sketch of the proof

Let $k > 2$ be an odd positive integer. Consider the system of equations

$$a_1 x + n = u^k$$
$$a_2 x + n = v^k.$$ 

Let $\alpha = (a_1/a_2)^{1/k}$. Then,

$$n(a_2 - a_1) = a_2 u^k - a_1 v^k = a_2 \prod_{j=0}^{k-1} (u - \alpha \zeta_k^j v)$$

$$= a_2 (u - \alpha v) \prod_{j=1}^{(k-1)/2} |u - \alpha \zeta_k^j v|^2 \geq a_2 |u - \alpha v| |\alpha|^{k-1} v^{k-1} \prod_{j=1}^{(k-1)/2} \left( \sin \frac{2\pi j}{k} \right)^2,$$

which roughly says

$$\left| \frac{u}{v} - \alpha \right| \leq \frac{a_2}{v^k}.$$
The gap principle

Let \((u_i, v_i)\) are a set of solutions of the above system of equations. Then,

\[
\frac{1}{v_i v_{i+1}} \leq \left| \frac{u_i}{v_i} - \frac{u_{i+1}}{v_{i+1}} \right| \leq \left| \frac{u_i}{v_i} - \alpha \right| + \left| \alpha - \frac{u_{i+1}}{v_{i+1}} \right| \leq \frac{2a_2}{v_i^k}.
\]

Thus,

\[
v_{i+1} \geq \frac{v_i^{k-1}}{2a_2}, \quad v_{i+2} \geq \frac{v_{i+1}^{k-1}}{2a_2} \geq \frac{v_i^{2(k-1)}}{(2a_2)^k},
\]

and similarly

\[
v_{i+l} \geq \frac{v_i^{l(k-1)}}{(2a_2)^{(l-1)(k-1)+1}}.
\]

In other words, if \(a_i \geq n^L\) for \(L > 0\), then there is a \(\theta > 0\) such that

\[
v_i \gg n^{i\theta}.
\]
The ABC conjecture

Conjecture (Masser, Oesterlé)

Let \( \text{rad}(n) \) denote the product of distinct prime divisors of \( n \). Given \( \epsilon > 0 \), there exists a constant \( K_\epsilon \) such that the following holds: for all positive co-prime integers \( A, B \) and \( C \) with \( A + B = C \), we have

\[
C < K_\epsilon \text{rad}(ABC)^{1+\epsilon}.
\]
Applying ABC to

\[ a_1 v^k = n(a_2 - a_1) + a_2 u^k, \]

we get

\[ a_1 v^k \ll \operatorname{rad}(a_2 a_1 uvn(a_2 - a_1))^{1+\epsilon} \leq (a_2^3 v^2 n)^{1+\epsilon}. \]

Since \( k \geq 3 \), there exists a \( \kappa > 0 \) such that

\[ |v| \leq \max(n, a_2)^\kappa. \quad (2) \]

Comparing (1) and (2), we conclude

\[ M_k(n; L) \ll 1. \]
Without ABC conjecture

The proof relies on showing that there are fewer rational approximations of \( \alpha = \left(\frac{a_1}{a_2}\right)^{1/k} \),

\[ \left| \frac{u}{v} - \alpha \right| \leq \frac{a_2}{v^k}. \]

**Theorem (Roth)**

*Let \( \alpha \) be an algebraic irrational number. For every \( \epsilon > 0 \), there are finitely many \( (p, q) = 1 \) such that*

\[ \left| \alpha - \frac{p}{q} \right| \leq \frac{1}{q^{2+\epsilon}}. \]
Without ABC conjecture

**Theorem (Corvaja)**

Let $\alpha$ be an irrational algebraic integer of degree $k$ over $\mathbb{Q}$. Let $m > \max(9 \log k, 1000)$ be an integer such that $p_1/q_1, \cdots, p_m/q_m$ satisfy

$$\left| \alpha - \frac{p_i}{q_i} \right| \leq \frac{1}{q_i^{\kappa}}$$

for $\kappa > 2$. Further, suppose $q_{i+1} > q_i^\mu$, where $\mu = 2km^2m!$. Then,

$$\kappa < \frac{2}{1 - \frac{3\sqrt{\log k}}{\sqrt{m}}} + \frac{\log(2|\alpha| + 2)}{\log q_1} \frac{3m}{m!}.$$
Thank you for your attention!