Diophantine quadruples

Greg Martin
University of British Columbia
joint work with Scott Sitar

New York Number Theory Seminar
April 29, 2010
Outline

1. Introduction
2. Equidistribution
3. Reducible Quadratics
4. Final Calculation
Diophantine $m$-tuples

**Definition**

A *Diophantine $m$-tuple* is a set of $m$ positive integers 

$$\{a_1, a_2, \ldots, a_m\}$$

such that

$$a_ia_j + 1 \text{ is a perfect square}$$

for all $i \neq j$.

**Example (Fermat)**

$\{1, 3, 8, 120\}$ is a Diophantine quadruple, since

$$1 \cdot 3 + 1 = 2^2 \quad 1 \cdot 8 + 1 = 3^2 \quad 1 \cdot 120 + 1 = 11^2$$

$$3 \cdot 8 + 1 = 5^2 \quad 3 \cdot 120 + 1 = 19^2 \quad 8 \cdot 120 + 1 = 31^2.$$
Diophantine $m$-tuples

**Definition**

A Diophantine $m$-tuple is a set of $m$ positive integers

$$\{a_1, a_2, \ldots, a_m\}$$

such that

$$a_ia_j + 1$$

is a perfect square

for all $i \neq j$.

**Example (Fermat)**

$\{1, 3, 8, 120\}$ is a Diophantine quadruple, since

$$1 \cdot 3 + 1 = 2^2 \quad 1 \cdot 8 + 1 = 3^2 \quad 1 \cdot 120 + 1 = 11^2$$

$$3 \cdot 8 + 1 = 5^2 \quad 3 \cdot 120 + 1 = 19^2 \quad 8 \cdot 120 + 1 = 31^2.$$
Qualitative results

In terms of existence of Diophantine $m$-tuples, we know that there are:

- infinitely many Diophantine pairs (for example, $\{1, n^2 - 1\}$);
- infinitely many Diophantine triples and quadruples (known to Euler);
- finitely many Diophantine 5-tuples (Dujella), although it is expected that there are none;
- no Diophantine 6-tuples (Dujella), hence no Diophantine 7-tuples, 8-tuples, etc.

For the cases $m = 2, 3, 4$, we should therefore try to count the number of Diophantine $m$-tuples below some given bound $N$. 
Qualitative results

In terms of existence of Diophantine $m$-tuples, we know that there are:

- infinitely many Diophantine pairs (for example, $\{1, n^2 - 1\}$);
- infinitely many Diophantine triples and quadruples (known to Euler);
- finitely many Diophantine 5-tuples (Dujella), although it is expected that there are none;
- no Diophantine 6-tuples (Dujella), hence no Diophantine 7-tuples, 8-tuples, etc.

For the cases $m = 2, 3, 4$, we should therefore try to count the number of Diophantine $m$-tuples below some given bound $N$. 
Qualitative results

In terms of existence of Diophantine $m$-tuples, we know that there are:

- infinitely many Diophantine pairs (for example, $\{1, n^2 - 1\}$);
- infinitely many Diophantine triples and quadruples (known to Euler);
- finitely many Diophantine 5-tuples (Dujella), although it is expected that there are none;
- no Diophantine 6-tuples (Dujella), hence no Diophantine 7-tuples, 8-tuples, etc.

For the cases $m = 2, 3, 4$, we should therefore try to count the number of Diophantine $m$-tuples below some given bound $N$. 
Qualitative results

In terms of existence of Diophantine $m$-tuples, we know that there are:

- infinitely many Diophantine pairs (for example, $\{1, n^2 - 1\}$);
- infinitely many Diophantine triples and quadruples (known to Euler);
- finitely many Diophantine 5-tuples (Dujella), although it is expected that there are none;
- no Diophantine 6-tuples (Dujella), hence no Diophantine 7-tuples, 8-tuples, etc.

For the cases $m = 2, 3, 4$, we should therefore try to count the number of Diophantine $m$-tuples below some given bound $N$. 
Qualitative results

In terms of existence of Diophantine $m$-tuples, we know that there are:

- infinitely many Diophantine pairs (for example, $\{1, n^2 - 1\}$);
- infinitely many Diophantine triples and quadruples (known to Euler);
- finitely many Diophantine 5-tuples (Dujella), although it is expected that there are none;
- no Diophantine 6-tuples (Dujella), hence no Diophantine 7-tuples, 8-tuples, etc.

For the cases $m = 2, 3, 4$, we should therefore try to count the number of Diophantine $m$-tuples below some given bound $N$. 
Quantitative results

Let $D_m(N)$ be the number of Diophantine $m$-tuples contained in \{1, \ldots, N\}. Dujella (Ramanujan J., 2008) obtained:

- an asymptotic formula for $D_2(N)$;
- an asymptotic formula for $D_3(N)$;
- upper and lower bounds for $D_4(N)$ of the same order of magnitude.

Our contribution

We develop a method to obtain an asymptotic formula for $D_4(N)$. (Arguably, the method is even more interesting than the asymptotic formula.)

We first summarize the arguments for pairs and triples, which we will use as a starting point for studying quadruples.
Quantitative results

Let $D_m(N)$ be the number of Diophantine $m$-tuples contained in \{1, \ldots, N\}. Dujella (Ramanujan J., 2008) obtained:

- an asymptotic formula for $D_2(N)$;
- an asymptotic formula for $D_3(N)$;
- upper and lower bounds for $D_4(N)$ of the same order of magnitude.

Our contribution

We develop a method to obtain an asymptotic formula for $D_4(N)$. (Arguably, the method is even more interesting than the asymptotic formula.)

We first summarize the arguments for pairs and triples, which we will use as a starting point for studying quadruples.
Quantitative results

Let $D_m(N)$ be the number of Diophantine $m$-tuples contained in \{1, \ldots, N\}. Dujella (Ramanujan J., 2008) obtained:

- an asymptotic formula for $D_2(N)$;
- an asymptotic formula for $D_3(N)$;
- upper and lower bounds for $D_4(N)$ of the same order of magnitude.

Our contribution

We develop a method to obtain an asymptotic formula for $D_4(N)$. (Arguably, the method is even more interesting than the asymptotic formula.)

We first summarize the arguments for pairs and triples, which we will use as a starting point for studying quadruples.
Let $D_m(N)$ be the number of Diophantine $m$-tuples contained in $\{1, \ldots, N\}$. Dujella (Ramanujan J., 2008) obtained:

- an asymptotic formula for $D_2(N)$;
- an asymptotic formula for $D_3(N)$;
- upper and lower bounds for $D_4(N)$ of the same order of magnitude.

Our contribution

We develop a method to obtain an asymptotic formula for $D_4(N)$. (Arguably, the method is even more interesting than the asymptotic formula.)

We first summarize the arguments for pairs and triples, which we will use as a starting point for studying quadruples.
Quantitative results

Let $D_m(N)$ be the number of Diophantine $m$-tuples contained in \{1, \ldots, N\}. Dujella (Ramanujan J., 2008) obtained:

- an asymptotic formula for $D_2(N)$;
- an asymptotic formula for $D_3(N)$;
- upper and lower bounds for $D_4(N)$ of the same order of magnitude.

Our contribution

We develop a method to obtain an asymptotic formula for $D_4(N)$. (Arguably, the method is even more interesting than the asymptotic formula.)

We first summarize the arguments for pairs and triples, which we will use as a starting point for studying quadruples.
Counting Diophantine pairs

If \( \{a, b\} \) is a Diophantine pair, there exists an integer \( r \) such that
\[
ab + 1 = r^2,
\]
which implies that
\[
r^2 \equiv 1 \pmod{b}.
\]

Conversely, any solution of this congruence with \( 1 < r \leq b \) gives a Diophantine pair \( (\frac{r^2-1}{b}, b) \). (Note: \( r = 1 \) is excluded since it yields \( a = 0 \).)

Using this bijection

\[
D_2(N) = \text{number of Diophantine pairs in } \{1, \ldots, N\}
= \sum_{b \leq N} \#\{1 < r \leq b : r^2 \equiv 1 \pmod{b}\}
= \frac{6}{\pi^2} N \log N + O(N).
\]
Counting Diophantine pairs

If \( \{a, b\} \) is a Diophantine pair, there exists an integer \( r \) such that \( ab + 1 = r^2 \), which implies that

\[
r^2 \equiv 1 \pmod{b}.
\]

Conversely, any solution of this congruence with \( 1 < r \leq b \) gives a Diophantine pair \( (\frac{r^2 - 1}{b}, b) \). (Note: \( r = 1 \) is excluded since it yields \( a = 0 \).)

Using this bijection

\[
D_2(N) = \text{number of Diophantine pairs in } \{1, \ldots, N\}
= \sum_{b \leq N} \# \{1 < r \leq b : r^2 \equiv 1 \pmod{b}\}
= \frac{6}{\pi^2} N \log N + O(N).
\]
Counting Diophantine pairs

If \( \{a, b\} \) is a Diophantine pair, there exists an integer \( r \) such that \( ab + 1 = r^2 \), which implies that

\[
r^2 \equiv 1 \pmod{b}.
\]

Conversely, any solution of this congruence with \( 1 < r \leq b \) gives a Diophantine pair \( (\frac{r^2-1}{b}, b) \). (Note: \( r = 1 \) is excluded since it yields \( a = 0 \).)

Using this bijection

\[
D_2(N) = \text{number of Diophantine pairs in } \{1, \ldots, N\}
\]

\[
= \sum_{b \leq N} \#\{1 < r \leq b : r^2 \equiv 1 \pmod{b}\}
\]

\[
= \frac{6}{\pi^2} N \log N + O(N).
\]
Counting Diophantine pairs

If \( \{a, b\} \) is a Diophantine pair, there exists an integer \( r \) such that \( ab + 1 = r^2 \), which implies that

\[
r^2 \equiv 1 \pmod{b}.
\]

Conversely, any solution of this congruence with \( 1 < r \leq b \) gives a Diophantine pair \( \left( \frac{r^2 - 1}{b}, b \right) \). (Note: \( r = 1 \) is excluded since it yields \( a = 0 \).)

Using this bijection

\[
D_2(N) = \text{number of Diophantine pairs in } \{1, \ldots, N\}
\]

\[
= \sum_{b \leq N} \# \{ 1 < r \leq b : r^2 \equiv 1 \pmod{b} \}
\]

\[
= \frac{6}{\pi^2} N \log N + O(N).
\]
Counting Diophantine pairs

If \( \{a, b\} \) is a Diophantine pair, there exists an integer \( r \) such that \( ab + 1 = r^2 \), which implies that

\[
r^2 \equiv 1 \pmod{b}.
\]

Conversely, any solution of this congruence with \( 1 < r \leq b \) gives a Diophantine pair \( (\frac{r^2-1}{b}, b) \). (Note: \( r = 1 \) is excluded since it yields \( a = 0 \).)

Using this bijection

\[
D_2(N) = \text{number of Diophantine pairs in } \{1, \ldots, N\}
\]

\[
= \sum_{b \leq N} \#\{1 < r \leq b: r^2 \equiv 1 \pmod{b}\}
\]

\[
= \frac{6}{\pi^2} N \log N + O(N).
\]
Counting Diophantine pairs

If \( \{a, b\} \) is a Diophantine pair, there exists an integer \( r \) such that \( ab + 1 = r^2 \), which implies that

\[
r^2 \equiv 1 \pmod{b}.
\]

Conversely, any solution of this congruence with \( 1 < r \leq b \) gives a Diophantine pair \( (\frac{r^2-1}{b}, b) \). (Note: \( r = 1 \) is excluded since it yields \( a = 0 \).)

Using this bijection

\[
D_2(N) = \text{number of Diophantine pairs in } \{1, \ldots, N\}
= \sum_{b \leq N} \#\{1 < r \leq b : r^2 \equiv 1 \pmod{b}\}
= \frac{6}{\pi^2} N \log N + O(N).
\]
Regular Diophantine triples

Lemma

If \( \{a, b\} \) is a Diophantine pair, then

\[ \{a, b, a + b + 2r\} \]

is a Diophantine triple, where \( ab + 1 = r^2 \).

Proof.

Simply verify that \( a(a + b + 2r) + 1 = (a + r)^2 \) and
\[ b(a + b + 2r) + 1 = (b + r)^2. \]

Not all Diophantine triples arise in this way, but those that do are called regular. Those that do not are called irregular.
Regular Diophantine triples

**Lemma**

*If \( \{a, b\} \) is a Diophantine pair, then*

\[ \{a, b, a + b + 2r\} \]

*is a Diophantine triple, where \( ab + 1 = r^2 \).*

**Proof.**

Simply verify that:

- \( a(a + b + 2r) + 1 = (a + r)^2 \)
- \( b(a + b + 2r) + 1 = (b + r)^2 \).

Not all Diophantine triples arise in this way, but those that do are called *regular*. Those that do not are called *irregular*. 
Regular Diophantine triples

Lemma

If \( \{a, b\} \) is a Diophantine pair, then

\[ \{a, b, a + b + 2r\} \]

is a Diophantine triple, where \( ab + 1 = r^2 \).

Proof.

Simply verify that \( a(a + b + 2r) + 1 = (a + r)^2 \) and
\[ b(a + b + 2r) + 1 = (b + r)^2. \]

Not all Diophantine triples arise in this way, but those that do are called regular. Those that do not are called irregular.
Counting Diophantine triples

By elementary but complicated reasoning, Dujella showed that there are at most $cN$ irregular Diophantine triples in $\{1, \ldots, N\}$ (for some constant $c$).

Using the bijection between Diophantine pairs $\{a, b\}$ and pairs $\{b, r\}$ where $r^2 \equiv 1 \pmod{b}$, a similar counting argument establishes an asymptotic formula for the number of regular Diophantine triples in $\{1, \ldots, N\}$.

**Theorem (Dujella)**

$$D_3(N) = \text{number of Diophantine triples in } \{1, \ldots, N\}$$

$$= \frac{3}{\pi^2} N \log N + O(N).$$
Counting Diophantine triples

- By elementary but complicated reasoning, Dujella showed that there are at most $cN$ irregular Diophantine triples in \{1, \ldots, N\} (for some constant $c$).

- Using the bijection between Diophantine pairs \{a, b\} and pairs \{b, r\} where $r^2 \equiv 1 \pmod{b}$, a similar counting argument establishes an asymptotic formula for the number of regular Diophantine triples in \{1, \ldots, N\}.

**Theorem (Dujella)**

$$D_3(N) = \text{number of Diophantine triples in } \{1, \ldots, N\}$$

$$= \frac{3}{\pi^2} N \log N + O(N).$$
Counting Diophantine triples

- By elementary but complicated reasoning, Dujella showed that there are at most $cN$ irregular Diophantine triples in $\{1, \ldots, N\}$ (for some constant $c$).
- Using the bijection between Diophantine pairs $\{a, b\}$ and pairs $\{b, r\}$ where $r^2 \equiv 1 \pmod{b}$, a similar counting argument establishes an asymptotic formula for the number of regular Diophantine triples in $\{1, \ldots, N\}$.

**Theorem (Dujella)**

$$D_3(N) = \text{number of Diophantine triples in } \{1, \ldots, N\}$$

$$= \frac{3}{\pi^2} N \log N + O(N).$$
Regular Diophantine quadruples

Lemma (Arkin, Hoggatt, and Strauss, 1979)

If \( \{a, b, c\} \) is a Diophantine triple, then

\[
\{a, b, c, a + b + c + 2abc + 2rst\}
\]

is a Diophantine quadruple, where

\[
ab + 1 = r^2, \quad ac + 1 = s^2, \quad \text{and} \quad bc + 1 = t^2.
\]

Not all Diophantine quadruples arise in this way, but those that do are called regular.
Regular Diophantine quadruples

**Lemma (Arkin, Hoggatt, and Strauss, 1979)**

If \( \{a, b, c\} \) is a Diophantine triple, then

\[
\{a, b, c, a + b + c + 2abc + 2rst\}
\]

is a Diophantine quadruple, where

\[
ab + 1 = r^2, \quad ac + 1 = s^2, \quad \text{and} \quad bc + 1 = t^2.
\]

Not all Diophantine quadruples arise in this way, but those that do are called regular.
Regular Diophantine quadruples

Lemma (Arkin, Hoggatt, and Strauss, 1979)

If \( \{a, b, c\} \) is a Diophantine triple, then

\[
\{a, b, c, a + b + c + 2abc + 2rst\}
\]

is a Diophantine quadruple, where

\[
ab + 1 = r^2, \quad ac + 1 = s^2, \quad \text{and} \quad bc + 1 = t^2.
\]

Not all Diophantine quadruples arise in this way, but those that do are called regular.
Doubly regular Diophantine quadruples

What happens if we start with a Diophantine pair \( \{a, b\} \) (with \( ab + 1 = r^2 \)), then form the regular Diophantine triple \( \{a, b, a + b + 2r\} \), then use the lemma on the previous slide to form a Diophantine quadruple?

**Lemma (known to Euler)**

If \( \{a, b\} \) is a Diophantine pair, then

\[
\{a, b, a + b + 2r, 4r(a + r)(b + r)\}
\]

is a Diophantine quadruple, where \( ab + 1 = r^2 \).

Diophantine quadruples that arise in this way are called *doubly regular*. 
Doubly regular Diophantine quadruples

What happens if we start with a Diophantine pair \( \{a, b\} \) (with \( ab + 1 = r^2 \)), then form the regular Diophantine triple \( \{a, b, a + b + 2r\} \), then use the lemma on the previous slide to form a Diophantine quadruple?

**Lemma (known to Euler)**

If \( \{a, b\} \) is a Diophantine pair, then

\[
\{a, b, a + b + 2r, 4r(a + r)(b + r)\}
\]

is a Diophantine quadruple, where \( ab + 1 = r^2 \).

Diophantine quadruples that arise in this way are called doubly regular.
Doubly regular Diophantine quadruples

What happens if we start with a Diophantine pair \( \{a, b\} \) (with \( ab + 1 = r^2 \)), then form the regular Diophantine triple \( \{a, b, a + b + 2r\} \), then use the lemma on the previous slide to form a Diophantine quadruple?

**Lemma (known to Euler)**

*If \( \{a, b\} \) is a Diophantine pair, then*

\[
\{a, b, a + b + 2r, 4r(a + r)(b + r)\}
\]

*is a Diophantine quadruple, where \( ab + 1 = r^2 \).*

Diophantine quadruples that arise in this way are called *doubly regular.*
Counting Diophantine quadruples

It turns out that the main contribution to $D_4(N)$ comes from doubly regular quadruples: the number of non-doubly-regular Diophantine quadruples in $\{1, \ldots, N\}$ is $O(N^{1/3})$.

However, Dujella was not able to get a precise asymptotic formula for (doubly regular) Diophantine quadruples. Instead he got upper and lower bounds of the same order of magnitude:

Theorem (Dujella)

If $D_4(N)$ is the number of Diophantine quadruples in $\{1, \ldots, N\}$, then

$$0.1608 \cdot N^{1/3} \log N < D_4(N) < 0.5354 \cdot N^{1/3} \log N$$

when $N$ is sufficiently large.
Counting Diophantine quadruples

It turns out that the main contribution to $D_4(N)$ comes from doubly regular quadruples: the number of non-doubly-regular Diophantine quadruples in $\{1, \ldots, N\}$ is $O(N^{1/3})$.

However, Dujella was not able to get a precise asymptotic formula for (doubly regular) Diophantine quadruples. Instead he got upper and lower bounds of the same order of magnitude:

**Theorem (Dujella)**

If $D_4(N)$ is the number of Diophantine quadruples in $\{1, \ldots, N\}$, then

$$0.1608 \cdot N^{1/3} \log N < D_4(N) < 0.5354 \cdot N^{1/3} \log N$$

when $N$ is sufficiently large.
Counting Diophantine quadruples

It turns out that the main contribution to $D_4(N)$ comes from doubly regular quadruples: the number of non-doubly-regular Diophantine quadruples in $\{1, \ldots, N\}$ is $O(N^{1/3})$.

However, Dujella was not able to get a precise asymptotic formula for (doubly regular) Diophantine quadruples. Instead he got upper and lower bounds of the same order of magnitude:

**Theorem (Dujella)**

If $D_4(N)$ is the number of Diophantine quadruples in $\{1, \ldots, N\}$, then

$$0.1608 \cdot N^{1/3} \log N < D_4(N) < 0.5354 \cdot N^{1/3} \log N$$

when $N$ is sufficiently large.
Counting Diophantine Quadruples

Doubly regular Diophantine quadruples

\[ \{a, b, a + b + 2r, 4r(a + r)(b + r)\}, \text{ where } ab + 1 = r^2 \]

- As before, for each \( b \) we find all the solutions \( 1 < r \leq b \) to \( r^2 \equiv 1 \pmod{b} \); each solution determines \( a = \frac{r^2 - 1}{b} \).
- The obstacle to counting Diophantine quadruples in \( \{1, \ldots, N\} \): when \( b \) is around \( N^{1/3} \) in size (the most important range), whether or not \( 4r(a + r)(b + r) \) is less than \( N \) depends very much on how big \( r \) is relative to \( b \).

Our idea:

- Pretend that every such \( r \) is a random number between 1 and \( b \), and calculate what the asymptotic formula would be.
- Use the theory of equidistribution to prove that, on average, the solutions \( r \) really do behave randomly.
Counting Diophantine Quadruples

Doubly regular Diophantine quadruples

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

- As before, for each \(b\) we find all the solutions \(1 < r \leq b\) to \(r^2 \equiv 1 \pmod{b}\); each solution determines \(a = \frac{r^2 - 1}{b}\).
- The obstacle to counting Diophantine quadruples in \(\{1, \ldots, N\}\): when \(b\) is around \(N^{1/3}\) in size (the most important range), whether or not \(4r(a + r)(b + r)\) is less than \(N\) depends very much on how big \(r\) is relative to \(b\).

Our idea:
- Pretend that every such \(r\) is a random number between 1 and \(b\), and calculate what the asymptotic formula would be.
- Use the theory of equidistribution to prove that, on average, the solutions \(r\) really do behave randomly.
Counting Diophantine Quadruples

Doubly regular Diophantine quadruples

\[ \{a, b, a + b + 2r, 4r(a + r)(b + r)\}, \text{ where } ab + 1 = r^2 \]

- As before, for each \( b \) we find all the solutions \( 1 < r \leq b \) to \( r^2 \equiv 1 \pmod{b} \); each solution determines \( a = \frac{r^2 - 1}{b} \).
- The obstacle to counting Diophantine quadruples in \( \{1, \ldots, N\} \): when \( b \) is around \( N^{1/3} \) in size (the most important range), whether or not \( 4r(a + r)(b + r) \) is less than \( N \) depends very much on how big \( r \) is relative to \( b \).

Our idea:
- Pretend that every such \( r \) is a random number between 1 and \( b \), and calculate what the asymptotic formula would be.
- Use the theory of equidistribution to prove that, on average, the solutions \( r \) really do behave randomly.
Counting Diophantine Quadruples

Doubly regular Diophantine quadruples

\[ \{a, b, a + b + 2r, 4r(a + r)(b + r)\}, \text{ where } ab + 1 = r^2 \]

- As before, for each \( b \) we find all the solutions \( 1 < r \leq b \) to \( r^2 \equiv 1 \pmod{b} \); each solution determines \( a = \frac{r^2 - 1}{b} \).
- The obstacle to counting Diophantine quadruples in \( \{1, \ldots, N\} \): when \( b \) is around \( N^{1/3} \) in size (the most important range), whether or not \( 4r(a + r)(b + r) \) is less than \( N \) depends very much on how big \( r \) is relative to \( b \).

Our idea:
- Pretend that every such \( r \) is a random number between 1 and \( b \), and calculate what the asymptotic formula would be.
- Use the theory of equidistribution to prove that, on average, the solutions \( r \) really do behave randomly.
Counting Diophantine Quadruples

Doubly regular Diophantine quadruples

\[ \{a, b, a + b + 2r, 4r(a + r)(b + r)\}, \text{ where } ab + 1 = r^2 \]

- As before, for each \( b \) we find all the solutions \( 1 < r \leq b \) to \( r^2 \equiv 1 \pmod{b} \); each solution determines \( a = \frac{r^2 - 1}{b} \).
- The obstacle to counting Diophantine quadruples in \( \{1, \ldots, N\} \): when \( b \) is around \( N^{1/3} \) in size (the most important range), whether or not \( 4r(a + r)(b + r) \) is less than \( N \) depends very much on how big \( r \) is relative to \( b \).

Our idea:

- Pretend that every such \( r \) is a random number between 1 and \( b \), and calculate what the asymptotic formula would be.
- Use the theory of equidistribution to prove that, on average, the solutions \( r \) really do behave randomly.
Counting Diophantine Quadruples

Doubly regular Diophantine quadruples

\[ \{a, b, a + b + 2r, 4r(a + r)(b + r)\}, \text{ where } ab + 1 = r^2 \]

- As before, for each \( b \) we find all the solutions \( 1 < r \leq b \) to \( r^2 \equiv 1 \pmod{b} \); each solution determines \( a = \frac{r^2 - 1}{b} \).

- The obstacle to counting Diophantine quadruples in \( \{1, \ldots, N\} \): when \( b \) is around \( N^{1/3} \) in size (the most important range), whether or not \( 4r(a + r)(b + r) \) is less than \( N \) depends very much on how big \( r \) is relative to \( b \).

Our idea:
- Pretend that every such \( r \) is a random number between 1 and \( b \), and calculate what the asymptotic formula would be.
- Use the theory of equidistribution to prove that, on average, the solutions \( r \) really do behave randomly.
Introduction

**Equidistribution**

Given a sequence \( \{u_1, u_2, \ldots \} \) of real numbers between 0 and 1, define

\[
S(N; \alpha, \beta) = \# \{ i \leq N : \alpha \leq u_i \leq \beta \}.
\]

**Definition**

We say that the sequence is equidistributed modulo 1 if

\[
\lim_{N \to \infty} \frac{S(N; \alpha, \beta)}{N} = \beta - \alpha
\]

for all \( 0 \leq \alpha \leq \beta \leq 1 \).

In other words, every fixed interval \([\alpha, \beta]\) in \([0, 1]\) gets its fair share of the \(u_i\).
Equidistribution

Notation
Given a sequence \( \{u_1, u_2, \ldots \} \) of real numbers between 0 and 1, define

\[
S(N; \alpha, \beta) = \# \{ i \leq N : \alpha \leq u_i \leq \beta \}.
\]

Definition
We say that the sequence is equidistributed modulo 1 if

\[
\lim_{N \to \infty} \frac{S(N; \alpha, \beta)}{N} = \beta - \alpha
\]

for all \( 0 \leq \alpha \leq \beta \leq 1 \).

In other words, every fixed interval \([\alpha, \beta]\) in \([0, 1]\) gets its fair share of the \( u_i \).
Equidistribution

Notation

Given a sequence \( \{u_1, u_2, \ldots \} \) of real numbers between 0 and 1, define

\[
S(N; \alpha, \beta) = \#\{i \leq N: \alpha \leq u_i \leq \beta\}.
\]

Definition

We say that the sequence is equidistributed modulo 1 if

\[
\lim_{N \to \infty} \frac{S(N; \alpha, \beta)}{N} = \beta - \alpha
\]

for all \( 0 \leq \alpha \leq \beta \leq 1 \).

In other words, every fixed interval \([\alpha, \beta]\) in \([0, 1]\) gets its fair share of the \(u_i\).
Weyl’s criterion

Theorem (Weyl)

The sequence \( \{u_1, u_2, \ldots \} \) is equidistributed modulo 1 if and only if

\[
\lim_{n \to \infty} \frac{1}{n} \sum_{j=1}^{n} e^{2\pi i k u_j} = 0
\]

for every integer \( k \geq 1 \).

Intuitively, if the sequence is equidistributed modulo 1, we would expect enough cancellation in the sum to make the limit tend to 0.

Weyl’s criterion can be made quantitative, and the result is known as the Erdős-Turán inequality:
Weyl’s criterion

Theorem (Weyl)

The sequence \( \{u_1, u_2, \ldots \} \) is equidistributed modulo 1 if and only if

\[
\lim_{n \to \infty} \frac{1}{n} \sum_{j=1}^{n} e^{2\pi i k u_j} = 0
\]

for every integer \( k \geq 1 \).

Intuitively, if the sequence is equidistributed modulo 1, we would expect enough cancellation in the sum to make the limit tend to 0.

Weyl’s criterion can be made quantitative, and the result is known as the Erdős-Turán inequality:
Weyl’s criterion

Theorem (Weyl)

The sequence \( \{u_1, u_2, \ldots\} \) is equidistributed modulo 1 if and only if

\[
\lim_{n \to \infty} \frac{1}{n} \sum_{j=1}^{n} e^{2\pi i k u_j} = 0
\]

for every integer \( k \geq 1 \).

Intuitively, if the sequence is equidistributed modulo 1, we would expect enough cancellation in the sum to make the limit tend to 0.

Weyl’s criterion can be made quantitative, and the result is known as the Erdős-Turán inequality:
Weyl’s criterion

Theorem (Weyl)

The sequence \( \{u_1, u_2, \ldots \} \) is equidistributed modulo 1 if and only if

\[
\lim_{n \to \infty} \frac{1}{n} \sum_{j=1}^{n} e^{2\pi i k u_j} = 0
\]

for every integer \( k \geq 1 \).

Intuitively, if the sequence is equidistributed modulo 1, we would expect enough cancellation in the sum to make the limit tend to 0.

Weyl’s criterion can be made quantitative, and the result is known as the Erdős-Turán inequality:
The Erdős-Turán inequality

Definition

The discrepancy of the sequence \( \{u_1, u_2, \ldots \} \) is

\[
D(N; \alpha, \beta) = S(N; \alpha, \beta) - N(\beta - \alpha),
\]

where \( S(N; \alpha, \beta) = \#\{i \leq N : \alpha \leq u_i \leq \beta\} \).

Theorem (Erdős-Turán)

For any positive integers \( N \) and \( K \),

\[
|D(N; \alpha, \beta)| \leq \frac{N}{K + 1} + 2 \sum_{k=1}^{K} C(K, k) \left| \sum_{n=1}^{N} e^{2\pi i knu} \right|,
\]

where \( C(K, k) = \frac{1}{K+1} + \min (\beta - \alpha, \frac{1}{\pi k}) \).

Diophantine quadruples

Greg Martin
The Erdős-Turán inequality

**Definition**

The **discrepancy** of the sequence \( \{u_1, u_2, \ldots \} \) is

\[
D(N; \alpha, \beta) = S(N; \alpha, \beta) - N(\beta - \alpha),
\]

where \( S(N; \alpha, \beta) = \# \{i \leq N: \alpha \leq u_i \leq \beta\} \).

**Theorem (Erdős-Turán)**

*For any positive integers \( N \) and \( K \),*

\[
|D(N; \alpha, \beta)| \leq \frac{N}{K+1} + 2 \sum_{k=1}^{K} C(K, k) \left| \sum_{n=1}^{N} e^{2\pi i k u_n} \right|,
\]

*where \( C(K, k) = \frac{1}{K+1} + \min \left( \beta - \alpha, \frac{1}{\pi k} \right) \).*
The Erdős-Turán inequality

**Definition**

The discrepancy of the sequence \( \{u_1, u_2, \ldots \} \) is

\[
D(N; \alpha, \beta) = S(N; \alpha, \beta) - N(\beta - \alpha),
\]

where \( S(N; \alpha, \beta) = \#\{i \leq N : \alpha \leq u_i \leq \beta\} \).

**Theorem (Erdős-Turán)**

*For any positive integers \( N \) and \( K \),*

\[
|D(N; \alpha, \beta)| \leq \frac{N}{K + 1} + 2 \sum_{k=1}^{K} C(K, k) \left| \sum_{n=1}^{N} e^{2\pi i k u_n} \right|,
\]

*where \( C(K, k) = \frac{1}{K+1} + \min \left( \beta - \alpha, \frac{1}{\pi k} \right) \).*
What if the target interval moves?

Let $\alpha = \{\alpha_1, \alpha_2, \ldots \}$ and $\beta = \{\beta_1, \beta_2, \ldots \}$ be the endpoints of a sequence of intervals $[\alpha_i, \beta_i]$.

**Notation, version 2.0**

Define the counting function

$$S(N; \alpha, \beta) = \#\{i \leq N : \alpha_i \leq u_i \leq \beta_i\}.$$ 

and the discrepancy

$$D(N; \alpha, \beta) = S(N; \alpha, \beta) - \sum_{n=1}^{N} (\beta_n - \alpha_n).$$

An existing proof of the original Erdős-Turán inequality can be adapted to account for these moving target intervals $[\alpha_i, \beta_i]$:
What if the target interval moves?

Let \( \alpha = \{\alpha_1, \alpha_2, \ldots \} \) and \( \beta = \{\beta_1, \beta_2, \ldots \} \) be the endpoints of a sequence of intervals \([\alpha_i, \beta_i]\).

**Notation, version 2.0**

Define the **counting function**

\[
S(N; \alpha, \beta) = \#\{i \leq N: \alpha_i \leq u_i \leq \beta_i\}.
\]

and the **discrepancy**

\[
D(N; \alpha, \beta) = S(N; \alpha, \beta) - \sum_{n=1}^{N} (\beta_n - \alpha_n).
\]

An existing proof of the original Erdős-Turán inequality can be adapted to account for these moving target intervals \([\alpha_i, \beta_i]\):
What if the target interval moves?

Let \( \alpha = \{\alpha_1, \alpha_2, \ldots \} \) and \( \beta = \{\beta_1, \beta_2, \ldots \} \) be the endpoints of a sequence of intervals \([\alpha_i, \beta_i]\).

**Notation, version 2.0**

Define the counting function

\[
S(N; \alpha, \beta) = \#\{i \leq N : \alpha_i \leq u_i \leq \beta_i\}.
\]

and the discrepancy

\[
D(N; \alpha, \beta) = S(N; \alpha, \beta) - \sum_{n=1}^{N} (\beta_n - \alpha_n).
\]

An existing proof of the original Erdős-Turán inequality can be adapted to account for these moving target intervals \([\alpha_i, \beta_i]\):
What if the target interval moves?

Let $\alpha = \{\alpha_1, \alpha_2, \ldots \}$ and $\beta = \{\beta_1, \beta_2, \ldots \}$ be the endpoints of a sequence of intervals $[\alpha_i, \beta_i]$.

**Notation, version 2.0**

Define the counting function

$$S(N; \alpha, \beta) = \#\{i \leq N: \alpha_i \leq u_i \leq \beta_i\}.$$ 

and the discrepancy

$$D(N; \alpha, \beta) = S(N; \alpha, \beta) - \sum_{n=1}^{N} (\beta_n - \alpha_n).$$

An existing proof of the original Erdős-Turán inequality can be adapted to account for these moving target intervals $[\alpha_i, \beta_i]$. 

Diophantine quadruples

Greg Martin
Erdős-Turán with a moving target

**Theorem (M.-Sitar, 2010)**

For any $N$ and $K$, the discrepancy is bounded by

$$|D(N; \alpha, \beta)| \leq \frac{N}{K+1} + \sum_{k=1}^{K} C(K, k) \max_{1 \leq T \leq N} \left| \sum_{n=1}^{T} e^{2\pi i ku_n} \right|$$

$$\times \left( 1 + \sum_{n=1}^{N-1} |\alpha_{n+1} - \alpha_n| + \sum_{n=1}^{N-1} |\beta_{n+1} - \beta_n| \right),$$

where $C(K, k) = \frac{2-16/7\pi}{K+1} + \frac{16/7\pi}{k}$. 

Some dependence on $\alpha$ and $\beta$ is necessary: the target intervals $[\alpha_i, \beta_i]$ could be correlated with the sequence $\{u_i\}$ being counted.
Erdős-Turán with a moving target

**Theorem (M.-Sitar, 2010)**

For any $N$ and $K$, the discrepancy is bounded by

$$|D(N; \alpha, \beta)| \leq \frac{N}{K+1} + \sum_{k=1}^{K} C(K, k) \max_{1 \leq T \leq N} \left| \sum_{n=1}^{T} e^{2\pi iku_n} \right|$$

$$\times \left( 1 + \sum_{n=1}^{N-1} |\alpha_{n+1} - \alpha_n| + \sum_{n=1}^{N-1} |\beta_{n+1} - \beta_n| \right),$$

where $C(K, k) = \frac{2-16/7\pi}{K+1} + \frac{16/7\pi}{k}$.

Some dependence on $\alpha$ and $\beta$ is necessary: the target intervals $[\alpha_i, \beta_i]$ could be correlated with the sequence $\{u_i\}$ being counted.
Erdős-Turán with a moving target

**Theorem (M.-Sitar, 2010)**

For any $N$ and $K$, the discrepancy is bounded by

$$|D(N; \alpha, \beta)| \leq \frac{N}{K+1} + \sum_{k=1}^{K} C(K, k) \max_{1 \leq T \leq N} \left| \sum_{n=1}^{T} e^{2\pi i k u_n} \right|$$

$$\times \left( 1 + \sum_{n=1}^{N-1} |\alpha_{n+1} - \alpha_n| + \sum_{n=1}^{N-1} |\beta_{n+1} - \beta_n| \right),$$

where $C(K, k) = \frac{2-16/7\pi}{K+1} + \frac{16/7\pi}{k}$.

- Some dependence on $\alpha$ and $\beta$ is necessary: the target intervals $[\alpha_i, \beta_i]$ could be correlated with the sequence $\{u_i\}$ being counted.
One Step Down...

We have managed to prove one of the technical tools which we will need in our final calculation. However, remember that we were looking at tuples of the form

\[ \{a, b, a + b + 2r, 4r(a + r)(b + r)\}, \]

where we wish to ensure that

\[ 4r(a + r)(b + r) \leq N. \]

To do this, we will need to investigate the behaviour of the roots of the congruence \( r^2 - 1 \equiv 0 \pmod{b} \) as \( b \) varies, which brings us to our next tool.
Hooley’s Result

Given a polynomial $f(x) \in \mathbb{Z}[x]$, consider finding its roots modulo $n$ for each integer $n$, say $\{r_{n,1}, \ldots\}$. If we first normalize so that $0 \leq r_{n,i} < n$, and then divide each element $r_{n,i}$ by $n$, we get a sequence of numbers lying between 0 and 1.

In [2], Hooley showed that if $f$ is irreducible, then in fact the above sequence of answers modulo $n$, concatenated together, is equidistributed modulo 1.
For our application to Diophantine quadruples, we are interested in the case where $f(x) = x^2 - 1$, which is reducible. However, a slight modification to Hooley’s argument shows that the solution sequence coming from a (non-square) reducible quadratic is equidistributed modulo 1 as well.
Our Modification

Hooley’s argument starts by considering the function $\rho(n)$, which counts the number of solutions to

$$f(x) \equiv 0 \pmod{n}.$$  

After deriving some information about $\rho(n)$, he proceeds with his estimation. When only looking at reducible quadratics, however, much of this information can be obtained without needing to resort to his work.
Our Modification

To begin, Hooley notes that $\rho(n)$ has the following four properties:

- $\rho(n)$ is multiplicative,
- if $p \nmid \text{disc}(f)$, then $\rho(p) = \rho(p^\alpha) \leq \deg(f)$,
- $\rho(p^\alpha) = O(1)$,
- $\rho(n) = O((\deg(f))^{\omega(n)})$.

For reducible quadratics, these are all readily verified as well.
Our Modification

Hooley also needs an estimate on the sum

$$\sum_{\ell \leq x} \sqrt{\frac{\rho(\ell)}{\ell \phi(\ell)}}.$$  

Using results from the literature on average values of multiplicative functions, we can again accomplish this without needing to resort to Hooley’s argument.
Our Modification

If we define

\[ R(h, x) = \sum_{k \leq x} \sum_{f(v) \equiv 0 \pmod{k}} \sum_{0 < v \leq k} e^{2\pi i hv/k}, \]

then by running Hooley’s argument with our modifications, we obtain for \( h \neq 0 \) the estimate:

\[ |R(h, x)| < C(h)x(\log x)^{\sqrt{2}-1}(\log \log x)^{5/2}, \]

which implies equidistribution modulo 1 since \( R(h, x) \) is \( o(x \log x) \), the total number of roots considered in the above sums (up to an error term).
The inequality constraining $r$

For each $b$, we were trying to count the number of solutions to $r^2 \equiv 1 \pmod{b}$ which gave rise to $a$'s such that

$$4r(a + r)(b + r) \leq N.$$ 

Since $a = \frac{r^2 - 1}{b} \approx \frac{r^2}{b}$, this inequality is essentially equivalent to

$$4r \left( \left( \frac{r}{b} \right)^2 + \frac{r}{b} \right) \left( 1 + \frac{r}{b} \right) \leq \frac{N}{b^3},$$

which is equivalent to

$$\frac{r}{b} \leq \min \left\{ 1, \frac{1}{2} \left( \sqrt{\frac{2N^{1/2}}{b^{3/2}}} + 1 - 1 \right) \right\}.$$
The inequality constraining $r$

For each $b$, we were trying to count the number of solutions to $r^2 \equiv 1 \pmod{b}$ which gave rise to $a$’s such that

$$4r(a + r)(b + r) \leq N.$$ 

Since $a = \frac{r^2-1}{b} \approx \frac{r^2}{b}$, this inequality is essentially equivalent to

$$4 \frac{r}{b} ((\frac{r}{b})^2 + \frac{r}{b})(1 + \frac{r}{b}) \leq \frac{N}{b^3},$$

which is equivalent to

$$\frac{r}{b} \leq \min \left\{ 1, \frac{1}{2} \left( \sqrt{\frac{2N^{1/2}}{b^{3/2}}} + 1 - 1 \right) \right\}.$$
The inequality constraining $r$

For each $b$, we were trying to count the number of solutions to $r^2 \equiv 1 \pmod{b}$ which gave rise to $a$’s such that

$$4r(a + r)(b + r) \leq N.$$ 

Since $a = \frac{r^2 - 1}{b} \approx \frac{r^2}{b}$, this inequality is essentially equivalent to

$$4 \frac{r}{b} \left( (\frac{r}{b})^2 + \frac{r}{b} \right) (1 + \frac{r}{b}) \leq \frac{N}{b^3},$$

which is equivalent to

$$\frac{r}{b} \leq \min \left\{ 1, \frac{1}{2} \left( \sqrt{\frac{2N^{1/2}}{b^{3/2}}} + 1 - 1 \right) \right\}.$$
If the $r$ were random... 

We’ve determined that the number of doubly regular Diophantine quadruples is essentially

$$\sum_b \# \left\{ r \leq b : r^2 \equiv 1 \pmod{b}, \frac{r}{b} \leq \min \left\{ 1, \frac{1}{2} \left( \sqrt{\frac{2N^{1/2}}{b^3/2}} + 1 - 1 \right) \right\} \right\}.$$

If the solutions $r$ were randomly distributed between 1 and $b$, then this sum would equal

$$\sum_b \min \left\{ 1, \frac{1}{2} \left( \sqrt{\frac{2N^{1/2}}{b^3/2}} + 1 - 1 \right) \right\} \# \{ r \leq b : r^2 \equiv 1 \pmod{b} \} = \sum_b \min \left\{ 1, \frac{1}{2} \left( \sqrt{\frac{2N^{1/2}}{b^3/2}} + 1 - 1 \right) \right\} \rho(b).$$
If the \( r \) were random...

We’ve determined that the number of doubly regular Diophantine quadruples is essentially

\[
\sum_b \# \left\{ r \leq b : r^2 \equiv 1 \pmod{b}, \frac{r}{b} \leq \min \left\{ 1, \frac{1}{2} \left( \sqrt{\frac{2N^{1/2}}{b^{3/2}}} + 1 - 1 \right) \right\} \right\}.
\]

If the solutions \( r \) were randomly distributed between 1 and \( b \), then this sum would equal

\[
\sum_b \min \left\{ 1, \frac{1}{2} \left( \sqrt{\frac{2N^{1/2}}{b^{3/2}}} + 1 - 1 \right) \right\} \# \{ r \leq b : r^2 \equiv 1 \pmod{b} \}
\]

\[
= \sum_b \min \left\{ 1, \frac{1}{2} \left( \sqrt{\frac{2N^{1/2}}{b^{3/2}}} + 1 - 1 \right) \right\} \rho(b).
\]
If the $r$ were random...

We’ve determined that the number of doubly regular Diophantine quadruples is essentially

$$\sum_{b} \# \left\{ r \leq b : r^2 \equiv 1 \pmod{b}, \frac{r}{b} \leq \min \left\{ 1, \frac{1}{2} \left( \sqrt{\frac{2N^{1/2}}{b^{3/2}}} + 1 - 1 \right) \right\} \right\}.$$ 

If the solutions $r$ were randomly distributed between 1 and $b$, then this sum would equal

$$\sum_{b} \min \left\{ 1, \frac{1}{2} \left( \sqrt{\frac{2N^{1/2}}{b^{3/2}}} + 1 - 1 \right) \right\} \# \{ r \leq b : r^2 \equiv 1 \pmod{b} \}$$

$$= \sum_{b} \min \left\{ 1, \frac{1}{2} \left( \sqrt{\frac{2N^{1/2}}{b^{3/2}}} + 1 - 1 \right) \right\} \rho(b).$$
Random enough

In fact, the error is exactly the discrepancy $D(N; \alpha, \beta)$, where (for a suitable bound $B$):

$$\{ u_i \} = \bigcup_{b \leq B} \left\{ \frac{r}{b} : 1 < r \leq b, \ r^2 \equiv 1 \pmod{b} \right\}$$

$$\alpha_i = 0 \quad \text{and} \quad \beta_i = \min \left\{ 1, \frac{1}{2} \left( \sqrt{\frac{2N^{1/2}}{b^{3/2}}} + 1 - 1 \right) \right\}$$

- Erdős–Turán inequality with a moving target: the discrepancy is bounded in terms of exponential sums

$$\sum_{b \leq B} \sum_{1 < r \leq b} e^{2\pi i kr/b}.$$ 

- Equidistribution of roots of $r^2 - 1$: these exponential sums can be suitably bounded by the adaptation of Hooley’s method.
Random enough

In fact, the error is exactly the discrepancy $D(N; \alpha, \beta)$, where (for a suitable bound $B$):

$$\{u_i\} = \bigcup_{b \leq B} \{r/b : 1 < r \leq b, \ r^2 \equiv 1 \pmod{b}\}$$

$\alpha_i = 0$ and $\beta_i = \min \left\{1, \frac{1}{2} \left(\sqrt{\frac{2N^{1/2}}{b^{3/2}}} + 1 - 1\right)\right\}$

- Erdős–Turán inequality with a moving target: the discrepancy is bounded in terms of exponential sums

$$\sum_{b \leq B} \sum_{1 < r \leq b} e^{2\pi ikr/b}.$$  

- Equidistribution of roots of $r^2 - 1$: these exponential sums can be suitably bounded by the adaptation of Hooley’s method.
Random enough

In fact, the error is exactly the discrepancy $D(N; \alpha, \beta)$, where (for a suitable bound $B$):

$$\{u_i\} = \bigcup_{b \leq B} \left\{ \frac{r}{b} : 1 < r \leq b, \ r^2 \equiv 1 \pmod{b} \right\}$$

$$\alpha_i = 0 \quad \text{and} \quad \beta_i = \min \left\{ 1, \frac{1}{2} \left( \sqrt{\frac{2N^{1/2}}{b^{3/2}}} + 1 - 1 \right) \right\}$$

- Erdős–Turán inequality with a moving target: the discrepancy is bounded in terms of exponential sums

$$\sum_{b \leq B} \sum_{1 < r \leq b} e^{2\pi ikr/b}.$$  

- Equidistribution of roots of $r^2 - 1$: these exponential sums can be suitably bounded by the adaptation of Hooley’s method.
Putting the pieces together

Since the error is manageable, it remains only to evaluate

$$\sum_{b} \min \left\{ 1, \frac{1}{2} \left( \sqrt{\frac{2N^{1/2}}{b^{3/2}}} + 1 - 1 \right) \right\} \rho(b)$$

to count the number of doubly regular Diophantine quadruples.

**Theorem (M.-Sitar, 2010)**

The number of Diophantine quadruples in \( \{1, \ldots, N\} \) is

$$D_4(N) \sim CN^{1/3} \log N,$$

where

$$C = \frac{2^{4/3}}{3\Gamma(2/3)^3} \approx 0.33828 \ldots.$$
Putting the pieces together

Since the error is manageable, it remains only to evaluate

\[ \sum_{b} \min \left\{ 1, \frac{1}{2} \left( \sqrt{2^{N^{1/2}}/b^{3/2}} + 1 - 1 \right) \right\} \rho(b) \]

to count the number of doubly regular Diophantine quadruples.

**Theorem (M.-Sitar, 2010)**

The number of Diophantine quadruples in \( \{1, \ldots, N\} \) is

\[ D_4(N) \sim C N^{1/3} \log N, \]

where \( C = \frac{2^{4/3}}{3 \Gamma(2/3)^3} \approx 0.33828 \ldots \)

This is consistent with Dujella’s upper and lower bounds.
These slides

www.math.ubc.ca/~gerg/index.shtml?slides

Our paper “Erdős-Turán with a moving target, equidistribution of roots of reducible quadratics, and Diophantine quadruples”

www.math.ubc.ca/~gerg/

index.shtml?abstract=ETMTERRQDQ