Diophantine Quadruples

Greg Martin
University of British Columbia
joint work with Scott Sitar

Brigham Young University Number Theory Seminar
Provo, UT
May 24, 2011

Outline

Diophantine m-tuples

Definition

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

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

such that

$a_i a_j + 1$ is a perfect square

for all $i \neq j$.

Example (Fermat)

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

$$\begin{array}{ccc} 1 \cdot 3 + 1 = 2^2 & 1 \cdot 8 + 1 = 3^2 & 1 \cdot 120 + 1 = 11^2 \\ 3 \cdot 8 + 1 = 5^2 & 3 \cdot 120 + 1 = 19^2 & 8 \cdot 120 + 1 = 31^2. \end{array}$$

Diophantine m-tuples

Definition

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

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

such that

$$a_i a_j + 1 \text{ is a perfect square}$$

for all $i \neq j$.

Example (Fermat)

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

$$\begin{array}{ccc} 1 \cdot 3 + 1 = 2^2 & 1 \cdot 8 + 1 = 3^2 & 1 \cdot 120 + 1 = 11^2 \\ 3 \cdot 8 + 1 = 5^2 & 3 \cdot 120 + 1 = 19^2 & 8 \cdot 120 + 1 = 31^2. \end{array}$$

Qualitative results

In terms of existence of Diophatine 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 Diophatine 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 Diophatine 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 Diophatine 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 Diophatine 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 $\{1, \dots, N\}$. 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 $\{1, \dots, N\}$. 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 $\{1,\dots,N\}$. 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.

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

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

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 $1 < r \le b$ gives a Diophantine pair $(\frac{r^2-1}{b}, b)$. (Note: $r = 1$ is excluded since it yields $a = 0$.)

Using this bijection

$$\begin{aligned} D_2(N) &= \text{number of Diophantine pairs in } \{1, \dots, N\} \\ &= \sum_{b \le N} \#\{1 < r \le b \colon r^2 \equiv 1 \pmod{b}\} \\ &= \frac{6}{\pi^2} N \log N + O(N). \end{aligned}$$

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 $1 < r \le b$ gives a Diophantine pair $(\frac{r^2-1}{b}, b)$. (Note: $r = 1$ is excluded since it yields $a = 0$.)

Using this bijection

$$\begin{aligned} D_2(N) &= \text{number of Diophantine pairs in } \{1, \dots, N\} \\ &= \sum_{b \le N} \#\{1 < r \le b \colon r^2 \equiv 1 \pmod{b}\} \\ &= \frac{6}{\pi^2} N \log N + O(N). \end{aligned}$$

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 $1 < r \le b$ 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

$$\begin{aligned} D_2(N) &= \text{number of Diophantine pairs in } \{1, \dots, N\} \\ &= \sum_{b \le N} \#\{1 < r \le b \colon r^2 \equiv 1 \pmod{b}\} \\ &= \frac{6}{\pi^2} N \log N + O(N). \end{aligned}$$

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 $1<r\le b$ gives a Diophantine pair $(\frac{r^2-1}{b},b)$. (Note: $r=1$ is excluded since it yields $a=0$.)

Using this bijection

$$\begin{aligned} D_2(N) &= \text{number of Diophantine pairs in } \{1,\dots,N\} \\ &= \sum_{b\le N} \#\{1<r\le b\colon r^2\equiv 1 \pmod{b}\} \\ &= \frac{6}{\pi^2} N\log N + O(N). \end{aligned}$$

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 $1 < r \le b$ gives a Diophantine pair $(\frac{r^2-1}{b}, b)$. (Note: $r = 1$ is excluded since it yields $a = 0$.)

Using this bijection

$$\begin{aligned} D_2(N) &= \text{number of Diophantine pairs in } \{1, \dots, N\} \\ &= \sum_{b \le N} \#\{1 < r \le b \colon r^2 \equiv 1 \pmod{b}\} \\ &= \frac{6}{\pi^2} N \log N + O(N). \end{aligned}$$

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 $a(a + b + 2r) + 1 = (a + r)^2$ 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 $a(a + b + 2r) + 1 = (a + r)^2$ 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)

$$\begin{aligned} D_3(N) &= \textit{number of Diophantine triples in } \{1,\ldots,N\} \\ &= \frac{3}{\pi^2} N \log N + O(N). \end{aligned}$$

Counting Diophantine triples

- By elementary but complicated reasoning, Dujella showed that there are at most cN irregular Diophantine triples in $\{1,\dots,N\}$ (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 $\{1,\dots,N\}$.

Theorem (Dujella)

$$\begin{aligned} D_3(N) &= \text{number of Diophantine triples in } \{1,\dots,N\} \\ &= \frac{3}{\pi^2} N \log N + O(N). \end{aligned}$$

Counting Diophantine triples

- By elementary but complicated reasoning, Dujella showed that there are at most cN irregular Diophantine triples in $\{1, \dots, N\}$ (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 $\{1, \dots, N\}$.

Theorem (Dujella)

$$\begin{aligned} D_3(N) &= \textit{number of Diophantine triples in } \{1, \dots, N\} \\ &= \frac{3}{\pi^2} N \log N + O(N). \end{aligned}$$

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

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

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 $\{1,\dots,N\}$ 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 $\{1,\dots,N\}$,

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

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 $\{1, \dots, N\}$ 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 $\{1, \dots, N\}$,

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

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 $\{1,\dots,N\}$ 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 $\{1,\dots,N\}$,

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

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 $\{1,\dots,N\}$ 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 $\{1,\dots,N\}$,

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

when N is sufficiently large.

Guesses are welcome at this time

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 $1 < r \le b$ to $r^2 \equiv 1 \pmod{b}$; each solution determines $a = \frac{r^2-1}{b}$.
- The obstacle to counting Diophantine quadruples in $\{1, \dots, N\}$: 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 $1 < r \le b$ to $r^2 \equiv 1 \pmod{b}$; each solution determines $a = \frac{r^2-1}{b}$.
- The obstacle to counting Diophantine quadruples in $\{1, \dots, N\}$: 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 $1 < r \le b$ to $r^2 \equiv 1 \pmod{b}$; each solution determines $a = \frac{r^2-1}{b}$.
- The obstacle to counting Diophantine quadruples in $\{1, \dots, N\}$: 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 $1 < r \le b$ to $r^2 \equiv 1 \pmod{b}$; each solution determines $a = \frac{r^2-1}{b}$.
- The obstacle to counting Diophantine quadruples in $\{1, \dots, N\}$: 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 $\{1, \dots, N\}$: 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 $1 < r \le b$ to $r^2 \equiv 1 \pmod{b}$; each solution determines $a = \frac{r^2-1}{b}$.
- The obstacle to counting Diophantine quadruples in $\{1, \dots, N\}$: 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.

Equidistribution

Notation

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

$$S(N; \alpha, \beta) = \#\{i \le N \colon \alpha \le u_i \le \beta\}.$$

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 $0 \le \alpha \le \beta \le 1$.

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

$$S(N;\alpha,\beta) = \#\{i \le N \colon \alpha \le u_i \le \beta\}.$$

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 $0 \le \alpha \le \beta \le 1$.

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

$$S(N; \alpha, \beta) = \#\{i \le N \colon \alpha \le u_i \le \beta\}.$$

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 $0 \le \alpha \le \beta \le 1$.

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 $\{u_1, u_2, \dots\}$ *is equidistributed if and only if*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i k u_n} = 0$$

for every integer $k \geq 1$.

- Intuitively, if the sequence is equidistributed, 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 $\{u_1, u_2, \dots\}$ *is equidistributed if and only if*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i k u_n} = 0$$

for every integer $k \ge 1$.

- Intuitively, if the sequence is equidistributed, 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 $\{u_1, u_2, \dots\}$ *is equidistributed if and only if*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i k u_n} = 0$$

for every integer $k \ge 1$.

- Intuitively, if the sequence is equidistributed, 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 $\{u_1, u_2, \dots\}$ *is equidistributed if and only if*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i k u_n} = 0$$

for every integer $k \ge 1$.

- Intuitively, if the sequence is equidistributed, 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 $\{u_1, u_2, \dots\}$ is

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

where $S(N;\alpha,\beta) = \#\{i \le N \colon \alpha \le u_i \le \beta\}$.

Theorem (Erdős–Turán)

For any positive integers N and K,

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

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 $\{u_1, u_2, \dots\}$ is

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

where $S(N;\alpha,\beta) = \#\{i \le N \colon \alpha \le u_i \le \beta\}$.

Theorem (Erdős–Turán)

For any positive integers N and K,

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

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 $\{u_1, u_2, \dots\}$ is

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

where $S(N; \alpha, \beta) = \#\{i \le N \colon \alpha \le u_i \le \beta\}$.

Theorem (Erdős–Turán)

For any positive integers N and K,

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

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

What if the target interval moves?

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

Notation, version 2.0

Define the counting function

$$S(N; \boldsymbol{\alpha}, \boldsymbol{\beta}) = \#\{i \le N \colon \alpha_i \le u_i \le \beta_i\}.$$

and the discrepancy

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

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

Notation, version 2.0

Define the counting function

$$S(N; \boldsymbol{\alpha}, \boldsymbol{\beta}) = \#\{i \le N \colon \alpha_i \le u_i \le \beta_i\}.$$

and the discrepancy

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

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

Notation, version 2.0

Define the counting function

$$S(N; \boldsymbol{\alpha}, \boldsymbol{\beta}) = \#\{i \le N \colon \alpha_i \le u_i \le \beta_i\}.$$

and the discrepancy

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

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

Notation, version 2.0

Define the counting function

$$S(N; \boldsymbol{\alpha}, \boldsymbol{\beta}) = \#\{i \le N \colon \alpha_i \le u_i \le \beta_i\}.$$

and the discrepancy

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

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

Erdős–Turán with a moving target

Theorem (M.–Sitar, 2010)

For any N and K, the discrepancy is bounded by

$$|D(N;\boldsymbol{\alpha},\boldsymbol{\beta})| \le \frac{N}{K+1} + \sum_{k=1}^{K} C(K,k) \max_{1\le T\le N} \left| \sum_{n=1}^{T} e^{2\pi i k u_n} \right| \times \left(1 + \sum_{n=1}^{N-1} |\alpha_{n+1} - \alpha_n| + \sum_{n=1}^{N-1} |\beta_{n+1} - \beta_n| \right),$$

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

- Some dependence on α and β 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

$$|D(N;\boldsymbol{\alpha},\boldsymbol{\beta})| \le \frac{N}{K+1} + \sum_{k=1}^{K} C(K,k) \max_{1\le T\le N} \left| \sum_{n=1}^{T} e^{2\pi i k u_n} \right| \times \left(1 + \sum_{n=1}^{N-1} |\alpha_{n+1}-\alpha_n| + \sum_{n=1}^{N-1} |\beta_{n+1}-\beta_n| \right),$$

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

- Some dependence on α and β 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

$$|D(N;\boldsymbol{\alpha},\boldsymbol{\beta})| \le \frac{N}{K+1} + \sum_{k=1}^{K} C(K,k) \max_{1\le T\le N} \left| \sum_{n=1}^{T} e^{2\pi i k u_n} \right| \times \left(1 + \sum_{n=1}^{N-1} |\alpha_{n+1}-\alpha_n| + \sum_{n=1}^{N-1} |\beta_{n+1}-\beta_n| \right),$$

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

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

Moving targets can make the discrepancy large

Corollary

Suppose that $\{\alpha_n\}$ and $\{\beta_n\}$ are monotonic sequences. For any N and K, the discrepancy is bounded by

$$|D(N;\alpha,\beta)| \le \frac{N}{K} + \big(1 + |\alpha_N - \alpha_1| + |\beta_N - \beta_1|\big) \sum_{k=1}^{K} \max_{1\le T\le N} \left| \sum_{n=1}^{T} e^{2\pi i k u_n} \right| .$$

Notice that the discrepancy can easily be made to be about as large as N, by taking the "obliging target" intervals

$$\{\alpha_n\} = \{u_n - 2^{-n}\} \quad \text{and} \quad \{\beta_n\} = \{u_n + 2^{-n}\}.$$

Moving targets can make the discrepancy large

Corollary

Suppose that $\{\alpha_n\}$ and $\{\beta_n\}$ are monotonic sequences. For any N and K, the discrepancy is bounded by

$$|D(N;\alpha,\beta)| \le \frac{N}{K} + \big(1+|\alpha_N-\alpha_1|+|\beta_N-\beta_1|\big)\sum_{k=1}^{K}\max_{1\le T\le N}\left|\sum_{n=1}^{T} e^{2\pi i k u_n}\right|.$$

Notice that the discrepancy can easily be made to be about as large as N, by taking the “obliging target” intervals

$$\{\alpha_n\} = \{u_n - 2^{-n}\} \quad \text{and} \quad \{\beta_n\} = \{u_n + 2^{-n}\}.$$

Moving targets can make the discrepancy large

Corollary

Suppose that $\{\alpha_n\}$ and $\{\beta_n\}$ are monotonic sequences. For any N and K, the discrepancy is bounded by

$$|D(N;\alpha,\beta)| \le \frac{N}{K} + \left(1 + |\alpha_N - \alpha_1| + |\beta_N - \beta_1|\right) \sum_{k=1}^{K} \max_{1\le T\le N} \left| \sum_{n=1}^{T} e^{2\pi i k u_n} \right|.$$

Notice that the discrepancy can easily be made to be about as large as N, by taking the “obliging target” intervals

$$\{\alpha_n\} = \{u_n - 2^{-n}\} \quad \text{and} \quad \{\beta_n\} = \{u_n + 2^{-n}\}.$$

Our upper bound is reasonably tight

Example

Take $\{u_n\} = \{n^\gamma\}$ for some real number $0 < \gamma < 1$, with the "obliging target" intervals from the previous slide.

- $|\alpha_N - \alpha_1|$ and $|\beta_N - \beta_1|$ are about N^γ
- $\sum_{n=1}^{N} e(kn^\gamma)$ is asymptotic to $N^{1-\gamma} e(kN^\gamma)/(2\pi i k\gamma)$, which has order of magnitude $N^{1-\gamma}/k$

The upper bound becomes about

$$\frac{N}{K} + \sum_{k=1}^{K} N^\gamma \frac{N^{1-\gamma}}{k} \sim N \log K,$$

which does indeed allow for a discrepancy of N.

Our upper bound is reasonably tight

Example

Take $\{u_n\} = \{n^\gamma\}$ for some real number $0 < \gamma < 1$, with the "obliging target" intervals from the previous slide.

- $|\alpha_N - \alpha_1|$ and $|\beta_N - \beta_1|$ are about N^γ
- $\sum_{n=1}^{N} e(kn^\gamma)$ is asymptotic to $N^{1-\gamma} e(kN^\gamma)/(2\pi ik\gamma)$, which has order of magnitude $N^{1-\gamma}/k$

The upper bound becomes about

$$\frac{N}{K} + \sum_{k=1}^{K} N^\gamma \frac{N^{1-\gamma}}{k} \sim N \log K,$$

which does indeed allow for a discrepancy of N.

Our upper bound is reasonably tight

Example

Take $\{u_n\} = \{n^\gamma\}$ for some real number $0 < \gamma < 1$, with the "obliging target" intervals from the previous slide.

- $|\alpha_N - \alpha_1|$ and $|\beta_N - \beta_1|$ are about N^γ
- $\sum_{n=1}^N e(kn^\gamma)$ is asymptotic to $N^{1-\gamma}e(kN^\gamma)/(2\pi ik\gamma)$, which has order of magnitude $N^{1-\gamma}/k$

The upper bound becomes about

$$\frac{N}{K} + \sum_{k=1}^{K} N^\gamma \frac{N^{1-\gamma}}{k} \sim N \log K,$$

which does indeed allow for a discrepancy of N.

Our upper bound is reasonably tight

Example

Take $\{u_n\} = \{n^\gamma\}$ for some real number $0 < \gamma < 1$, with the "obliging target" intervals from the previous slide.

- $|\alpha_N - \alpha_1|$ and $|\beta_N - \beta_1|$ are about N^γ
- $\sum_{n=1}^N e(kn^\gamma)$ is asymptotic to $N^{1-\gamma} e(kN^\gamma)/(2\pi i k\gamma)$, which has order of magnitude $N^{1-\gamma}/k$

The upper bound becomes about

$$\frac{N}{K} + \sum_{k=1}^{K} N^\gamma \frac{N^{1-\gamma}}{k} \sim N \log K,$$

which does indeed allow for a discrepancy of N.

Normalized roots of polynomial congruences

What sequence of real numbers do we want to examine the equidistribution of?

Definition

Given a polynomial $f(t) \in \mathbb{Z}[t]$, we form the sequence

$$\bigcup_{m\ge1} \left\{ \tfrac{r}{m} : 0 \le r < m, f(r) \equiv 0 \pmod{m} \right\}.$$

Example

If $f(t) = t^2 - 19$, then the corresponding sequence of normalized roots is $\{\frac12, \frac13, \frac23, \frac25, \frac35, \frac16, \frac56, \frac19, \frac89, \frac{3}{10}, \frac{7}{10}, \frac{2}{15}, \frac{7}{15}, \frac{8}{15}, \frac{13}{15}, \dots\}$.

Normalized roots of polynomial congruences

What sequence of real numbers do we want to examine the equidistribution of?

Definition

Given a polynomial $f(t) \in \mathbb{Z}[t]$, we form the sequence

$$\bigcup_{m \ge 1} \left\{ \tfrac{r}{m} : 0 \le r < m, f(r) \equiv 0 \pmod{m} \right\}.$$

Example

If $f(t) = t^2 - 19$, then the corresponding sequence of normalized roots is $\{\frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{2}{5}, \frac{3}{5}, \frac{1}{6}, \frac{5}{6}, \frac{1}{9}, \frac{8}{9}, \frac{3}{10}, \frac{7}{10}, \frac{2}{15}, \frac{7}{15}, \frac{8}{15}, \frac{13}{15}, \dots\}$.

Normalized roots of polynomial congruences

What sequence of real numbers do we want to examine the equidistribution of?

Definition

Given a polynomial $f(t) \in \mathbb{Z}[t]$, we form the sequence

$$\bigcup_{m\ge1} \left\{ \tfrac{r}{m} : 0 \le r < m,\ f(r) \equiv 0 \pmod{m} \right\}.$$

Example

If $f(t) = t^2 - 19$, then the corresponding sequence of normalized roots is $\{\frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{2}{5}, \frac{3}{5}, \frac{1}{6}, \frac{5}{6}, \frac{1}{9}, \frac{8}{9}, \frac{3}{10}, \frac{7}{10}, \frac{2}{15}, \frac{7}{15}, \frac{8}{15}, \frac{13}{15}, \dots\}$.

Normalized roots of polynomial congruences

What sequence of real numbers do we want to examine the equidistribution of?

Definition

Given a polynomial $f(t) \in \mathbb{Z}[t]$, we form the sequence

$$\bigcup_{m\ge1} \left\{ \tfrac{r}{m} : 0 \le r < m, f(r) \equiv 0 \pmod{m} \right\}.$$

Example

If $f(t) = t^2 - 19$, then the corresponding sequence of normalized roots is $\{\frac12, \frac13, \frac23, \frac25, \frac35, \frac16, \frac56, \frac19, \frac89, \frac{3}{10}, \frac{7}{10}, \frac{2}{15}, \frac{7}{15}, \frac{8}{15}, \frac{13}{15}, \dots\}$.

Hooley's result

Theorem (Hooley, 1964)

If $f(t) \in \mathbb{Z}[t]$ is irreducible, then the sequence $\bigcup_{m\ge1} \left\{ \frac{r}{m} : 0 \le r < m,\, f(r) \equiv 0 \pmod{m} \right\}$ is equidistributed. In fact, if f has degree d, then

$$\sum_{m\le x} \sum_{\substack{0\le r<m \\ f(r)\equiv 0 \pmod{m}}} e^{2\pi ikr/m} \ll \frac{x}{(\log x)^{\sqrt{d}/d!}}$$

for any nonzero integer k. (The number of summands is $\asymp x$.)

For our application to Diophantine quadruples, we are interested in $f(t) = t^2 - 1$, which is reducible. We therefore need to modify Hooley's argument to show equidistribution of the corresponding sequence of normalized roots.

Hooley's result

Theorem (Hooley, 1964)

If $f(t) \in \mathbb{Z}[t]$ is irreducible, then the sequence $\bigcup_{m\ge1} \left\{ \frac{r}{m} : 0 \le r < m, f(r) \equiv 0 \pmod m \right\}$ is equidistributed. In fact, if f has degree d, then

$$\sum_{m\le x} \sum_{\substack{0\le r<m \\ f(r)\equiv 0 \pmod m}} e^{2\pi ikr/m} \ll \frac{x}{(\log x)^{\sqrt{d}/d!}}$$

for any nonzero integer k. (The number of summands is $\asymp x$.)

For our application to Diophantine quadruples, we are interested in $f(t) = t^2 - 1$, which is reducible. We therefore need to modify Hooley's argument to show equidistribution of the corresponding sequence of normalized roots.

Hooley's result

Theorem (Hooley, 1964)

If $f(t) \in \mathbb{Z}[t]$ is irreducible, then the sequence $\bigcup_{m\ge1}\left\{\frac{r}{m} : 0 \le r < m,\ f(r) \equiv 0 \pmod{m}\right\}$ is equidistributed. In fact, if f has degree d, then

$$\sum_{m\le x} \sum_{\substack{0\le r<m \\ f(r)\equiv 0 \pmod{m}}} e^{2\pi i k r/m} \ll \frac{x}{(\log x)^{\sqrt{d}/d!}}$$

for any nonzero integer k. (The number of summands is $\asymp x$.)

For our application to Diophantine quadruples, we are interested in $f(t) = t^2 - 1$, which is reducible. We therefore need to modify Hooley's argument to show equidistribution of the corresponding sequence of normalized roots.

Hooley's result

Theorem (Hooley, 1964)

If $f(t) \in \mathbb{Z}[t]$ is irreducible, then the sequence $\bigcup_{m\ge1} \left\{\frac{r}{m} : 0 \le r < m, f(r) \equiv 0 \pmod{m}\right\}$ is equidistributed. In fact, if f has degree d, then

$$\sum_{m\le x} \sum_{\substack{0\le r<m \\ f(r)\equiv 0 \pmod{m}}} e^{2\pi ikr/m} \ll \frac{x}{(\log x)^{\sqrt{d}/d!}}$$

for any nonzero integer k. (The number of summands is $\asymp x$.)

For our application to Diophantine quadruples, we are interested in $f(t) = t^2 - 1$, which is reducible. We therefore need to modify Hooley's argument to show equidistribution of the corresponding sequence of normalized roots.

Hooley's result

Theorem (Hooley, 1964)

If $f(t) \in \mathbb{Z}[t]$ is irreducible, then the sequence $\bigcup_{m\ge1} \left\{ \frac{r}{m} : 0 \le r < m, f(r) \equiv 0 \pmod m \right\}$ is equidistributed. In fact, if f has degree d, then

$$\sum_{m\le x} \sum_{\substack{0\le r<m \\ f(r)\equiv 0 \pmod m}} e^{2\pi i k r/m} \ll \frac{x}{(\log x)^{\sqrt{d}/d!}}$$

for any nonzero integer k. (The number of summands is $\asymp x$.)

For our application to Diophantine quadruples, we are interested in $f(t) = t^2 - 1$, which is reducible. We therefore need to modify Hooley's argument to show equidistribution of the corresponding sequence of normalized roots.

How much do we need to change?

Definition

$\rho(m)$ is the number of solutions to $f(x) \equiv 0 \pmod{m}$.

Hooley's argument has two main parts:

- Using combinatorial arguments (dividing integers according to whether they are divisible by large or small primes, for example) to isolate the essential inequalities needed bound the exponential sum

  We can use these arguments verbatim.

- Incorporating information about ρ to produce nontrivial upper bounds in those inequalities

  For $f(t) = t^2 - 1$, the function ρ behaves quite differently; on the other hand, we can calculate it explicitly.

How much do we need to change?

Definition

$\rho(m)$ is the number of solutions to $f(x) \equiv 0 \pmod{m}$.

Hooley's argument has two main parts:

- Using combinatorial arguments (dividing integers according to whether they are divisible by large or small primes, for example) to isolate the essential inequalities needed bound the exponential sum

  We can use these arguments verbatim.

- Incorporating information about ρ to produce nontrivial upper bounds in those inequalities

  For $f(t) = t^2 - 1$, the function ρ behaves quite differently; on the other hand, we can calculate it explicitly.

How much do we need to change?

Definition

$\rho(m)$ is the number of solutions to $f(x) \equiv 0 \pmod{m}$.

Hooley's argument has two main parts:

- Using combinatorial arguments (dividing integers according to whether they are divisible by large or small primes, for example) to isolate the essential inequalities needed bound the exponential sum

  We can use these arguments verbatim.

- Incorporating information about ρ to produce nontrivial upper bounds in those inequalities

  For $f(t) = t^2 - 1$, the function ρ behaves quite differently; on the other hand, we can calculate it explicitly.

How much do we need to change?

Definition

$\rho(m)$ is the number of solutions to $f(x) \equiv 0 \pmod{m}$.

Hooley's argument has two main parts:

- Using combinatorial arguments (dividing integers according to whether they are divisible by large or small primes, for example) to isolate the essential inequalities needed bound the exponential sum

  We can use these arguments verbatim.

- Incorporating information about ρ to produce nontrivial upper bounds in those inequalities

  For $f(t) = t^2 - 1$, the function ρ behaves quite differently; on the other hand, we can calculate it explicitly.

How much do we need to change?

Definition

$\rho(m)$ is the number of solutions to $f(x) \equiv 0 \pmod{m}$.

Hooley's argument has two main parts:

- Using combinatorial arguments (dividing integers according to whether they are divisible by large or small primes, for example) to isolate the essential inequalities needed bound the exponential sum

  We can use these arguments verbatim.

- Incorporating information about ρ to produce nontrivial upper bounds in those inequalities

  For $f(t) = t^2 - 1$, the function ρ behaves quite differently; on the other hand, we can calculate it explicitly.

What we need to know about ρ

Let d be the degree of f, and let Δ be the discriminant of f. Hooley notes that $\rho(m)$ has the following four properties:

- ρ is multiplicative (Chinese remainder theorem)
- if $p \nmid \Delta$, then $\rho(p) = \rho(p^\alpha) \le d$ for every $\alpha \ge 1$ (Hensel's lemma)
- $\rho(p^\alpha)$ is bounded uniformly in terms of Δ
- $\rho(m) \ll_f d^{\omega(m)}$, where $\omega(m)$ is the number of distinct prime factors of m

For $f(t) = t^2 - 1$, these properties are all readily verified as well. In fact, for any reducible quadratic f (not the square of a linear polynomial), we have $\rho(m) \le \sqrt{\Delta} \cdot 2^{\omega(m)}$:

What we need to know about ρ

Let d be the degree of f, and let Δ be the discriminant of f. Hooley notes that $\rho(m)$ has the following four properties:

- ρ is multiplicative (Chinese remainder theorem)
- if $p \nmid \Delta$, then $\rho(p) = \rho(p^\alpha) \le d$ for every $\alpha \ge 1$ (Hensel's lemma)
- $\rho(p^\alpha)$ is bounded uniformly in terms of Δ
- $\rho(m) \ll_f d^{\omega(m)}$, where $\omega(m)$ is the number of distinct prime factors of m

For $f(t) = t^2 - 1$, these properties are all readily verified as well. In fact, for any reducible quadratic f (not the square of a linear polynomial), we have $\rho(m) \le \sqrt{\Delta} \cdot 2^{\omega(m)}$:

What we need to know about ρ

Let d be the degree of f, and let Δ be the discriminant of f. Hooley notes that $\rho(m)$ has the following four properties:

- ρ is multiplicative (Chinese remainder theorem)
- if $p \nmid \Delta$, then $\rho(p) = \rho(p^\alpha) \le d$ for every $\alpha \ge 1$ (Hensel's lemma)
- $\rho(p^\alpha)$ is bounded uniformly in terms of Δ
- $\rho(m) \ll_f d^{\omega(m)}$, where $\omega(m)$ is the number of distinct prime factors of m

For $f(t) = t^2 - 1$, these properties are all readily verified as well. In fact, for any reducible quadratic f (not the square of a linear polynomial), we have $\rho(m) \le \sqrt{\Delta} \cdot 2^{\omega(m)}$:

What we need to know about ρ

Let d be the degree of f, and let Δ be the discriminant of f. Hooley notes that $\rho(m)$ has the following four properties:

- ρ is multiplicative (Chinese remainder theorem)
- if $p \nmid \Delta$, then $\rho(p) = \rho(p^\alpha) \le d$ for every $\alpha \ge 1$ (Hensel's lemma)
- $\rho(p^\alpha)$ is bounded uniformly in terms of Δ
- $\rho(m) \ll_f d^{\omega(m)}$, where $\omega(m)$ is the number of distinct prime factors of m

For $f(t) = t^2 - 1$, these properties are all readily verified as well. In fact, for any reducible quadratic f (not the square of a linear polynomial), we have $\rho(m) \le \sqrt{\Delta} \cdot 2^{\omega(m)}$:

What we need to know about ρ

Let d be the degree of f, and let Δ be the discriminant of f. Hooley notes that $\rho(m)$ has the following four properties:

- ρ is multiplicative (Chinese remainder theorem)
- if $p \nmid \Delta$, then $\rho(p) = \rho(p^\alpha) \le d$ for every $\alpha \ge 1$ (Hensel's lemma)
- $\rho(p^\alpha)$ is bounded uniformly in terms of Δ
- $\rho(m) \ll_f d^{\omega(m)}$, where $\omega(m)$ is the number of distinct prime factors of m

For $f(t) = t^2 - 1$, these properties are all readily verified as well. In fact, for any reducible quadratic f (not the square of a linear polynomial), we have $\rho(m) \le \sqrt{\Delta} \cdot 2^{\omega(m)}$:

What we need to know about ρ

Let d be the degree of f, and let Δ be the discriminant of f. Hooley notes that $\rho(m)$ has the following four properties:

- ρ is multiplicative (Chinese remainder theorem)
- if $p \nmid \Delta$, then $\rho(p) = \rho(p^\alpha) \le d$ for every $\alpha \ge 1$ (Hensel's lemma)
- $\rho(p^\alpha)$ is bounded uniformly in terms of Δ
- $\rho(m) \ll_f d^{\omega(m)}$, where $\omega(m)$ is the number of distinct prime factors of m

For $f(t) = t^2 - 1$, these properties are all readily verified as well. In fact, for any reducible quadratic f (not the square of a linear polynomial), we have $\rho(m) \le \sqrt{\Delta} \cdot 2^{\omega(m)}$:

The exact values of ρ

Lemma

Let $g(t) = (at+b)(ct+d)$ where $(a,b) = (c,d) = 1$ and $ad \neq bc$. Let p be a prime, and let $\delta = \operatorname{ord}_p(ad-bc)$. Then for any positive integer α, the number of roots of $g(t)$ modulo p^α is

$$\rho(p^\alpha) = \begin{cases} 2, & \text{if } p \nmid ac(ad-bc), \\ 0, & \text{if } p \mid ac \text{ and } p \mid (ad-bc), \\ 1, & \text{if } p \mid ac \text{ and } p \nmid (ad-bc), \\ p^{\lfloor \alpha/2 \rfloor}, & \text{if } p \nmid ac \text{ and } p \mid (ad-bc) \text{ and } \alpha \leq 2\delta, \\ 2p^\delta, & \text{if } p \nmid ac \text{ and } p \mid (ad-bc) \text{ and } \alpha > 2\delta. \end{cases}$$

In particular, $\rho(p^\alpha) \leq 2p^\delta$.

Since $\Delta = (ad-bc)^2$, this implies $\rho(m) \leq 2^{\omega(m)}\sqrt{\Delta}$.

The exact values of ρ

Lemma

Let $g(t) = (at+b)(ct+d)$ where $(a,b) = (c,d) = 1$ and $ad \ne bc$. Let p be a prime, and let $\delta = \operatorname{ord}_p(ad-bc)$. Then for any positive integer α, the number of roots of $g(t)$ modulo p^α is

$$\rho(p^\alpha) = \begin{cases} 2, & \text{if } p \nmid ac(ad-bc), \\ 0, & \text{if } p \mid ac \text{ and } p \mid (ad-bc), \\ 1, & \text{if } p \mid ac \text{ and } p \nmid (ad-bc), \\ p^{\lfloor \alpha/2 \rfloor}, & \text{if } p \nmid ac \text{ and } p \mid (ad-bc) \text{ and } \alpha \le 2\delta, \\ 2p^\delta, & \text{if } p \nmid ac \text{ and } p \mid (ad-bc) \text{ and } \alpha > 2\delta. \end{cases}$$

In particular, $\rho(p^\alpha) \le 2p^\delta$.

Since $\Delta = (ad-bc)^2$, this implies $\rho(m) \le 2^{\omega(m)}\sqrt{\Delta}$.

The exact values of ρ

Lemma

Let $g(t) = (at+b)(ct+d)$ where $(a,b) = (c,d) = 1$ and $ad \neq bc$. Let p be a prime, and let $\delta = \operatorname{ord}_p(ad-bc)$. Then for any positive integer α, the number of roots of $g(t)$ modulo p^α is

$$\rho(p^\alpha) = \begin{cases} 2, & \text{if } p \nmid ac(ad-bc), \\ 0, & \text{if } p \mid ac \text{ and } p \mid (ad-bc), \\ 1, & \text{if } p \mid ac \text{ and } p \nmid (ad-bc), \\ p^{\lfloor \alpha/2 \rfloor}, & \text{if } p \nmid ac \text{ and } p \mid (ad-bc) \text{ and } \alpha \le 2\delta, \\ 2p^\delta, & \text{if } p \nmid ac \text{ and } p \mid (ad-bc) \text{ and } \alpha > 2\delta. \end{cases}$$

In particular, $\rho(p^\alpha) \le 2p^\delta$.

Since $\Delta = (ad-bc)^2$, this implies $\rho(m) \le 2^{\omega(m)}\sqrt{\Delta}$.

The exact values of ρ

Lemma

Let $g(t) = (at+b)(ct+d)$ where $(a,b) = (c,d) = 1$ and $ad \neq bc$. Let p be a prime, and let $\delta = \mathrm{ord}_p(ad-bc)$. Then for any positive integer α, the number of roots of $g(t)$ modulo p^α is

$$\rho(p^\alpha) = \begin{cases} 2, & \text{if } p \nmid ac(ad-bc), \\ 0, & \text{if } p \mid ac \text{ and } p \mid (ad-bc), \\ 1, & \text{if } p \mid ac \text{ and } p \nmid (ad-bc), \\ p^{\lfloor \alpha/2 \rfloor}, & \text{if } p \nmid ac \text{ and } p \mid (ad-bc) \text{ and } \alpha \le 2\delta, \\ 2p^\delta, & \text{if } p \nmid ac \text{ and } p \mid (ad-bc) \text{ and } \alpha > 2\delta. \end{cases}$$

In particular, $\rho(p^\alpha) \le 2p^\delta$.

Since $\Delta = (ad-bc)^2$, this implies $\rho(m) \le 2^{\omega(m)}\sqrt{\Delta}$.

One key sum

Definition

$\rho(m)$ is the number of solutions to $f(x) \equiv 0 \pmod{m}$.

Hooley's method also requires an estimate for $\sum_{\ell \le x} \sqrt{\rho(\ell) \frac{\ell}{\phi(\ell)}}$.

Rule of thumb

If f is a nice multiplicative function such that $f(p)$ is β on average, then $\sum_{\ell \le x} f(\ell) \sim c(f) x (\log x)^{\beta - 1}$.

Since $\sqrt{\rho(p) \frac{p}{\phi(p)}} = \sqrt{2 \frac{p}{p-1}}$ for all but finitely many primes p when f is a reducible quadratic, we can take $\beta = \sqrt{2}$.

One key sum

Definition

$\rho(m)$ is the number of solutions to $f(x) \equiv 0 \pmod{m}$.

Hooley's method also requires an estimate for $\sum_{\ell \le x} \sqrt{\rho(\ell)\frac{\ell}{\phi(\ell)}}$.

Rule of thumb

If f is a nice multiplicative function such that $f(p)$ is β on average, then $\sum_{\ell \le x} f(\ell) \sim c(f)x(\log x)^{\beta-1}$.

Since $\sqrt{\rho(p)\frac{p}{\phi(p)}} = \sqrt{2\frac{p}{p-1}}$ for all but finitely many primes p when f is a reducible quadratic, we can take $\beta = \sqrt{2}$.

One key sum

Definition

$\rho(m)$ is the number of solutions to $f(x) \equiv 0 \pmod{m}$.

Hooley's method also requires an estimate for $\sum_{\ell \le x} \sqrt{\rho(\ell)\frac{\ell}{\phi(\ell)}}$.

Rule of thumb

If f is a nice multiplicative function such that $f(p)$ is β on average, then $\sum_{\ell \le x} f(\ell) \sim c(f)x(\log x)^{\beta-1}$.

Since $\sqrt{\rho(p)\frac{p}{\phi(p)}} = \sqrt{2\frac{p}{p-1}}$ for all but finitely many primes p when f is a reducible quadratic, we can take $\beta = \sqrt{2}$.

Our modification of Hooley's result

Theorem (M.–Sitar, 2010)

If $f(t) \in \mathbb{Z}[t]$ is a reducible quadratic (not a square), then the sequence $\bigcup_{m\geq 1}\left\{\frac{r}{m} : 0 \leq r < m, f(r) \equiv 0 \pmod{m}\right\}$ is equidistributed. In fact,

$$\sum_{m\leq x} \sum_{\substack{0\leq r<m \\ f(r)\equiv 0 \pmod{m}}} e^{2\pi ikr/m} \ll_{f,k} x(\log x)^{\sqrt{2}-1}(\log\log x)^{5/2}$$

for any nonzero integer k. (The number of summands is $\asymp x\log x$.)

Remark

The log-power savings might seem meager; however, we expect that the true order of magnitude of the exponential sum is $\asymp x$, due to the two roots of f that are present for most moduli.

Our modification of Hooley's result

Theorem (M.–Sitar, 2010)

If $f(t) \in \mathbb{Z}[t]$ is a reducible quadratic (not a square), then the sequence $\bigcup_{m\ge1} \left\{ \frac{r}{m} : 0 \le r < m,\, f(r) \equiv 0 \pmod m \right\}$ is equidistributed. In fact,

$$\sum_{m\le x} \sum_{\substack{0\le r<m \\ f(r)\equiv 0 \pmod m}} e^{2\pi i k r/m} \ll_{f,k} x(\log x)^{\sqrt{2}-1}(\log\log x)^{5/2}$$

for any nonzero integer k. (The number of summands is $\asymp x\log x$.)

Remark

The log-power savings might seem meager; however, we expect that the true order of magnitude of the exponential sum is $\asymp x$, due to the two roots of f that are present for most moduli.

Our modification of Hooley's result

Theorem (M.–Sitar, 2010)

If $f(t) \in \mathbb{Z}[t]$ *is a reducible quadratic (not a square), then the sequence* $\bigcup_{m\geq 1} \left\{ \frac{r}{m} : 0 \leq r < m, f(r) \equiv 0 \pmod{m} \right\}$ *is equidistributed. In fact,*

$$\sum_{m\leq x} \sum_{\substack{0\leq r<m \\ f(r)\equiv 0 \pmod{m}}} e^{2\pi ikr/m} \ll_{f,k} x(\log x)^{\sqrt{2}-1}(\log\log x)^{5/2}$$

for any nonzero integer k*. (The number of summands is* $\asymp x \log x$*.)*

Remark

The log-power savings might seem meager; however, we expect that the true order of magnitude of the exponential sum is $\asymp x$, due to the two roots of f that are present for most moduli.

Our modification of Hooley's result

Theorem (M.–Sitar, 2010)

If $f(t) \in \mathbb{Z}[t]$ is a reducible quadratic (not a square), then the sequence $\bigcup_{m\ge1} \left\{ \frac{r}{m} : 0 \le r < m, f(r) \equiv 0 \pmod m \right\}$ is equidistributed. In fact,

$$\sum_{m\le x} \sum_{\substack{0\le r<m \\ f(r)\equiv 0 \pmod m}} e^{2\pi i k r/m} \ll_{f,k} x(\log x)^{\sqrt{2}-1} (\log\log x)^{5/2}$$

for any nonzero integer k. (The number of summands is $\asymp x \log x$.)

Remark

The log-power savings might seem meager; however, we expect that the true order of magnitude of the exponential sum is $\asymp x$, due to the two roots of f that are present for most moduli.

Our modification of Hooley's result

Theorem (M.–Sitar, 2010)

If $f(t) \in \mathbb{Z}[t]$ is a reducible quadratic (not a square), then the sequence $\bigcup_{m\ge1} \left\{ \frac{r}{m} : 0 \le r < m,\, f(r) \equiv 0 \pmod{m} \right\}$ is equidistributed. In fact,

$$\sum_{m\le x} \sum_{\substack{0\le r<m \\ f(r)\equiv 0 \pmod{m}}} e^{2\pi ikr/m} \ll_{f,k} x(\log x)^{\sqrt{2}-1}(\log\log x)^{5/2}$$

for any nonzero integer k. (The number of summands is $\asymp x\log x$.)

Remark

The log-power savings might seem meager; however, we expect that the true order of magnitude of the exponential sum is $\asymp x$, due to the two roots of f that are present for most moduli.

What is the true size?

Example

With $f(t) = t^2 - 1$,

$$\sum_{m \le x} \sum_{\substack{0 \le r < m \\ f(r) \equiv 0 \ (\mathrm{mod}\ m)}} e^{2\pi i k r/m} = \sum_{m \le x} \left(e^{2\pi i k/m} + e^{2\pi i k(m-1)/m} \right) + \sum_{m \le x} \sum_{\substack{1 < r < m-1 \\ f(r) \equiv 0 \ (\mathrm{mod}\ m)}} e^{2\pi i k r/m}$$

$$= 2x + O(\log x) + (\text{random?}).$$

Conjecture

$$\sum_{m \le x} \sum_{\substack{0 \le r < m \\ r^2 - 1 \equiv 0 \ (\mathrm{mod}\ m)}} e^{2\pi i k r/m} = 2x + O(x^{1/2+\varepsilon})$$

What is the true size?

Example

With $f(t) = t^2 - 1$,

$$\sum_{m \le x} \sum_{\substack{0 \le r < m \\ f(r) \equiv 0 \pmod{m}}} e^{2\pi ikr/m} = \sum_{m \le x} \left(e^{2\pi ik/m} + e^{2\pi ik(m-1)/m} \right)$$

$$+ \sum_{m \le x} \sum_{\substack{1 < r < m-1 \\ f(r) \equiv 0 \pmod{m}}} e^{2\pi ikr/m}$$

$$= 2x + O(\log x) + (\text{random?}).$$

Conjecture

$$\sum_{m \le x} \sum_{\substack{0 \le r < m \\ r^2 - 1 \equiv 0 \pmod{m}}} e^{2\pi ikr/m} = 2x + O(x^{1/2+\varepsilon})$$

What is the true size?

Example

With $f(t) = t^2 - 1$,

$$\sum_{m \le x} \sum_{\substack{0 \le r < m \\ f(r) \equiv 0 \pmod{m}}} e^{2\pi i k r/m} = \sum_{m \le x} \left(e^{2\pi i k/m} + e^{2\pi i k(m-1)/m} \right) + \sum_{m \le x} \sum_{\substack{1 < r < m-1 \\ f(r) \equiv 0 \pmod{m}}} e^{2\pi i k r/m}$$

$$= 2x + O(\log x) + (\text{random?}).$$

Conjecture

$$\sum_{m \le x} \sum_{\substack{0 \le r < m \\ r^2 - 1 \equiv 0 \pmod{m}}} e^{2\pi i k r/m} = 2x + O(x^{1/2+\varepsilon})$$

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

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

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

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

which is equivalent to

$$\frac{r}{b} \le \min\Big\{1, \frac{1}{2}\Big(\sqrt{\frac{2N^{1/2}}{b^{3/2}} + 1} - 1\Big)\Big\}.$$

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

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

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

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

which is equivalent to

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

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

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

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

$$4\tfrac{r}{b}\big((\tfrac{r}{b})^2 + \tfrac{r}{b}\big)\big(1 + \tfrac{r}{b}\big) \le \tfrac{N}{b^3},$$

which is equivalent to

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

If the r were random...

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

$$\sum_b \#\left\{r \le b \colon r^2 \equiv 1 \pmod b,\ \tfrac{r}{b} \le \min\left\{1, \tfrac12\left(\sqrt{\tfrac{2N^{1/2}}{b^{3/2}}+1}-1\right)\right\}\right\}.$$

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

$$\sum_b \min\left\{1, \tfrac12\left(\sqrt{\tfrac{2N^{1/2}}{b^{3/2}}+1}-1\right)\right\}\#\{r \le b \colon r^2 \equiv 1 \pmod b\}$$
$$= \sum_b \min\left\{1, \tfrac12\left(\sqrt{\tfrac{2N^{1/2}}{b^{3/2}}+1}-1\right)\right\}\rho(b).$$

If the r were random. . .

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

$$\sum_b \#\left\{r \le b \colon r^2 \equiv 1 \pmod{b},\ \tfrac{r}{b} \le \min\left\{1, \tfrac12\left(\sqrt{\tfrac{2N^{1/2}}{b^{3/2}}+1}-1\right)\right\}\right\}.$$

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

$$\sum_b \min\left\{1, \tfrac12\left(\sqrt{\tfrac{2N^{1/2}}{b^{3/2}}+1}-1\right)\right\}\#\{r \le b \colon r^2 \equiv 1 \pmod{b}\}$$

$$= \sum_b \min\left\{1, \tfrac12\left(\sqrt{\tfrac{2N^{1/2}}{b^{3/2}}+1}-1\right)\right\}\rho(b).$$

If the r were random...

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

$$\sum_b \#\left\{r \le b\colon r^2 \equiv 1 \pmod{b},\ \tfrac{r}{b} \le \min\left\{1, \tfrac12\left(\sqrt{\tfrac{2N^{1/2}}{b^{3/2}}+1}-1\right)\right\}\right\}.$$

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

$$\sum_b \min\left\{1, \tfrac12\left(\sqrt{\tfrac{2N^{1/2}}{b^{3/2}}+1}-1\right)\right\}\#\{r \le b\colon r^2 \equiv 1 \pmod{b}\}$$
$$= \sum_b \min\left\{1, \tfrac12\left(\sqrt{\tfrac{2N^{1/2}}{b^{3/2}}+1}-1\right)\right\}\rho(b).$$

Random enough

In fact, the difference between those two expressions is exactly the discrepancy $D(N;\boldsymbol{\alpha},\boldsymbol{\beta})$, where (for a suitable bound B):

$$\{u_i\} = \bigcup_{b\le B} \left\{ \tfrac{r}{b} \colon 1 < r \le b,\ r^2 \equiv 1 \pmod{b} \right\}$$

$$\alpha_i = 0 \qquad \text{and} \qquad \beta_i = \min\left\{1, \tfrac12\left(\sqrt{\frac{2N^{1/2}}{b^{3/2}}+1}-1\right)\right\}$$

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

$$\sum_{b\le B} \sum_{\substack{1<r\le b \\ r^2\equiv 1 \pmod{b}}} e^{2\pi i k r/b}.$$

- 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 difference between those two expressions is exactly the discrepancy $D(N;\boldsymbol{\alpha},\boldsymbol{\beta})$, where (for a suitable bound B):

$$\{u_i\} = \bigcup_{b\le B} \left\{ \tfrac{r}{b} \colon 1 < r \le b,\ r^2 \equiv 1 \pmod{b} \right\}$$

$$\alpha_i = 0 \qquad \text{and} \qquad \beta_i = \min\left\{1, \tfrac12\left(\sqrt{\tfrac{2N^{1/2}}{b^{3/2}}+1}-1\right)\right\}$$

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

$$\sum_{b\le B} \sum_{\substack{1<r\le b \\ r^2\equiv 1 \pmod{b}}} e^{2\pi i k r/b}.$$

- 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 difference between those two expressions is exactly the discrepancy $D(N;\boldsymbol{\alpha},\boldsymbol{\beta})$, where (for a suitable bound B):

$$\{u_i\} = \bigcup_{b\le B} \left\{ \tfrac{r}{b} \colon 1 < r \le b,\ r^2 \equiv 1 \pmod{b} \right\}$$

$$\alpha_i = 0 \qquad \text{and} \qquad \beta_i = \min\left\{1, \tfrac12\left(\sqrt{\tfrac{2N^{1/2}}{b^{3/2}}+1}-1\right)\right\}$$

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

$$\sum_{b\le B} \sum_{\substack{1<r\le b \\ r^2\equiv 1 \pmod{b}}} e^{2\pi i k r/b}.$$

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

The partial summation argument

Notation

$$S(y) = \sum_{b \le y} \rho(b) \sim \frac{6}{\pi^2} y \log y$$

Skipping several intermediate steps:

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

$$\sim \int_1^B \min\left\{1, \frac{1}{2}\left(\sqrt{\frac{2N^{1/2}}{t^{3/2}} + 1} - 1\right)\right\} dS(t)$$

$$\sim \frac{3N^{1/2}}{4} \int_{(N/16)^{1/3}}^{\infty} \left(1 + \frac{2N^{1/2}}{t^{3/2}}\right)^{-1/2} \frac{S(t)}{t^{5/2}}\, dt$$

$$\sim \frac{2^{2/3}}{\pi^2} N^{1/3} \log N \int_0^1 (1+8u)^{-1/2} u^{-2/3}\, du.$$

The partial summation argument

Notation

$$S(y) = \sum_{b \le y} \rho(b) \sim \tfrac{6}{\pi^2} y \log y$$

Skipping several intermediate steps:

$$\sum_{b \le B} \min\left\{1, \tfrac12\left(\sqrt{\tfrac{2N^{1/2}}{b^{3/2}} + 1} - 1\right)\right\}\rho(b)$$

$$\sim \int_1^B \min\left\{1, \tfrac12\left(\sqrt{\tfrac{2N^{1/2}}{t^{3/2}} + 1} - 1\right)\right\} dS(t)$$

$$\sim \frac{3N^{1/2}}{4} \int_{(N/16)^{1/3}}^{\infty} \left(1 + \frac{2N^{1/2}}{t^{3/2}}\right)^{-1/2} \frac{S(t)}{t^{5/2}}\, dt$$

$$\sim \frac{2^{2/3}}{\pi^2} N^{1/3} \log N \int_0^1 (1 + 8u)^{-1/2} u^{-2/3}\, du.$$

The partial summation argument

Notation

$$S(y) = \sum_{b \le y} \rho(b) \sim \tfrac{6}{\pi^2} y \log y$$

Skipping several intermediate steps:

$$\begin{aligned}
\sum_{b \le B} \min\left\{1, \tfrac{1}{2}\left(\sqrt{\tfrac{2N^{1/2}}{b^{3/2}} + 1} - 1\right)\right\}\rho(b) \\
&\sim \int_1^B \min\left\{1, \tfrac{1}{2}\left(\sqrt{\tfrac{2N^{1/2}}{t^{3/2}} + 1} - 1\right)\right\} dS(t) \\
&\sim \frac{3N^{1/2}}{4} \int_{(N/16)^{1/3}}^{\infty} \left(1 + \frac{2N^{1/2}}{t^{3/2}}\right)^{-1/2} \frac{S(t)}{t^{5/2}}\, dt \\
&\sim \frac{2^{2/3}}{\pi^2} N^{1/3} \log N \int_0^1 (1+8u)^{-1/2} u^{-2/3}\, du.
\end{aligned}$$

The partial summation argument

Notation

$$S(y) = \sum_{b \le y} \rho(b) \sim \tfrac{6}{\pi^2} y \log y$$

Skipping several intermediate steps:

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

$$\sim \int_1^B \min\left\{1, \tfrac{1}{2}\left(\sqrt{\tfrac{2N^{1/2}}{t^{3/2}}+1}-1\right)\right\} dS(t)$$

$$\sim \frac{3N^{1/2}}{4} \int_{(N/16)^{1/3}}^{\infty} \left(1+\frac{2N^{1/2}}{t^{3/2}}\right)^{-1/2} \frac{S(t)}{t^{5/2}}\,dt$$

$$\sim \frac{2^{2/3}}{\pi^2} N^{1/3} \log N \int_0^1 (1+8u)^{-1/2} u^{-2/3}\,du.$$

The partial summation argument

Notation

$$S(y) = \sum_{b \le y} \rho(b) \sim \tfrac{6}{\pi^2} y \log y$$

Skipping several intermediate steps:

$$\begin{aligned}
\sum_{b \le B} \min\left\{1, \tfrac12\left(\sqrt{\tfrac{2N^{1/2}}{b^{3/2}}+1}-1\right)\right\}\rho(b) \\
&\sim \int_1^B \min\left\{1, \tfrac12\left(\sqrt{\tfrac{2N^{1/2}}{t^{3/2}}+1}-1\right)\right\} dS(t) \\
&\sim \frac{3N^{1/2}}{4} \int_{(N/16)^{1/3}}^{\infty} \left(1+\frac{2N^{1/2}}{t^{3/2}}\right)^{-1/2} \frac{S(t)}{t^{5/2}}\, dt \\
&\sim \frac{2^{2/3}}{\pi^2} N^{1/3} \log N \int_0^1 (1+8u)^{-1/2} u^{-2/3}\, du.
\end{aligned}$$

A lovely constant

Abramowitz and Stegun's *Handbook* allows us to evaluate the leading constant using hypergeometric functions:

$$\frac{2^{2/3}}{\pi^2}\int_0^1 (1+8u)^{-1/2}u^{-2/3}\,du = \frac{3\cdot 2^{2/3}}{\pi^2}\,{}_2F_1\big(\tfrac12,\tfrac13,\tfrac43;-8\big) \qquad (15.3.1)$$

$$= \frac{3\cdot 2^{2/3}}{\pi^2}\,{}_2F_1\big(1,\tfrac23,\tfrac43;-1\big) \qquad (15.3.22)$$

$$= \frac{1}{2^{1/3}\pi^{3/2}}\frac{\Gamma(\frac13)}{\Gamma(\frac56)} \qquad (15.1.21)$$

$$= \frac{1}{2^{2/3}\pi^2}\frac{\Gamma(\frac13)^2}{\Gamma(\frac23)} \qquad (6.1.18\ (\text{duplication}))$$

$$= \frac{2^{4/3}}{3\Gamma(\frac23)^3} \approx 0.338285. \qquad (6.1.17\ (\text{reflection}))$$

A lovely constant

Abramowitz and Stegun's *Handbook* allows us to evaluate the leading constant using hypergeometric functions:

$$\frac{2^{2/3}}{\pi^2}\int_0^1 (1+8u)^{-1/2}u^{-2/3}\,du = \frac{3\cdot 2^{2/3}}{\pi^2}{}_2F_1\left(\tfrac12,\tfrac13,\tfrac43;-8\right) \quad (15.3.1)$$

$$= \frac{3\cdot 2^{2/3}}{\pi^2}{}_2F_1\left(1,\tfrac23,\tfrac43;-1\right) \quad (15.3.22)$$

$$= \frac{1}{2^{1/3}\pi^{3/2}}\frac{\Gamma(\frac13)}{\Gamma(\frac56)} \quad (15.1.21)$$

$$= \frac{1}{2^{2/3}\pi^2}\frac{\Gamma(\frac13)^2}{\Gamma(\frac23)} \quad (6.1.18\text{ (duplication)})$$

$$= \frac{2^{4/3}}{3\Gamma(\frac23)^3} \approx 0.338285. \quad (6.1.17\text{ (reflection)})$$

A lovely constant

Abramowitz and Stegun's *Handbook* allows us to evaluate the leading constant using hypergeometric functions:

$$\frac{2^{2/3}}{\pi^2}\int_0^1 (1+8u)^{-1/2}u^{-2/3}\,du = \frac{3\cdot 2^{2/3}}{\pi^2}\,{}_2F_1\big(\tfrac12,\tfrac13,\tfrac43;-8\big) \quad (15.3.1)$$

$$= \frac{3\cdot 2^{2/3}}{\pi^2}\,{}_2F_1\big(1,\tfrac23,\tfrac43;-1\big) \quad (15.3.22)$$

$$= \frac{1}{2^{1/3}\pi^{3/2}}\frac{\Gamma(\frac13)}{\Gamma(\frac56)} \quad (15.1.21)$$

$$= \frac{1}{2^{2/3}\pi^2}\frac{\Gamma(\frac13)^2}{\Gamma(\frac23)} \quad \text{(6.1.18 (duplication))}$$

$$= \frac{2^{4/3}}{3\Gamma(\frac23)^3} \approx 0.338285. \quad \text{(6.1.17 (reflection))}$$

A lovely constant

Abramowitz and Stegun's *Handbook* allows us to evaluate the leading constant using hypergeometric functions:

$$\frac{2^{2/3}}{\pi^2}\int_0^1 (1+8u)^{-1/2}u^{-2/3}\,du = \frac{3\cdot 2^{2/3}}{\pi^2}\,{}_2F_1\left(\tfrac12,\tfrac13,\tfrac43;-8\right) \quad \text{(15.3.1)}$$

$$= \frac{3\cdot 2^{2/3}}{\pi^2}\,{}_2F_1\left(1,\tfrac23,\tfrac43;-1\right) \quad \text{(15.3.22)}$$

$$= \frac{1}{2^{1/3}\pi^{3/2}}\frac{\Gamma(\frac13)}{\Gamma(\frac56)} \quad \text{(15.1.21)}$$

$$= \frac{1}{2^{2/3}\pi^2}\frac{\Gamma(\frac13)^2}{\Gamma(\frac23)} \quad \text{(6.1.18 (duplication))}$$

$$= \frac{2^{4/3}}{3\Gamma(\frac23)^3} \approx 0.338285. \quad \text{(6.1.17 (reflection))}$$

A lovely constant

Abramowitz and Stegun's *Handbook* allows us to evaluate the leading constant using hypergeometric functions:

$$\frac{2^{2/3}}{\pi^2}\int_0^1 (1+8u)^{-1/2}u^{-2/3}\,du = \frac{3\cdot 2^{2/3}}{\pi^2}\,{}_2F_1\big(\tfrac12,\tfrac13,\tfrac43;-8\big) \qquad \text{(15.3.1)}$$

$$= \frac{3\cdot 2^{2/3}}{\pi^2}\,{}_2F_1\big(1,\tfrac23,\tfrac43;-1\big) \qquad \text{(15.3.22)}$$

$$= \frac{1}{2^{1/3}\pi^{3/2}}\frac{\Gamma(\frac13)}{\Gamma(\frac56)} \qquad \text{(15.1.21)}$$

$$= \frac{1}{2^{2/3}\pi^2}\frac{\Gamma(\frac13)^2}{\Gamma(\frac23)} \qquad \text{(6.1.18 (duplication))}$$

$$= \frac{2^{4/3}}{3\Gamma(\frac23)^3} \approx 0.338285. \qquad \text{(6.1.17 (reflection))}$$

A lovely constant

Abramowitz and Stegun's *Handbook* allows us to evaluate the leading constant using hypergeometric functions:

$$\begin{aligned}
\frac{2^{2/3}}{\pi^2}\int_0^1 (1+8u)^{-1/2}u^{-2/3}\,du &= \frac{3\cdot 2^{2/3}}{\pi^2}\,{}_2F_1\big(\tfrac12,\tfrac13,\tfrac43;-8\big) && \text{(15.3.1)}\\
&= \frac{3\cdot 2^{2/3}}{\pi^2}\,{}_2F_1\big(1,\tfrac23,\tfrac43;-1\big) && \text{(15.3.22)}\\
&= \frac{1}{2^{1/3}\pi^{3/2}}\frac{\Gamma(\frac13)}{\Gamma(\frac56)} && \text{(15.1.21)}\\
&= \frac{1}{2^{2/3}\pi^2}\frac{\Gamma(\frac13)^2}{\Gamma(\frac23)} && \text{(6.1.18 (duplication))}\\
&= \frac{2^{4/3}}{3\Gamma(\frac23)^3} \approx 0.338285. && \text{(6.1.17 (reflection))}
\end{aligned}$$

Putting the pieces together

Theorem (M.–Sitar, 2010)

The number of Diophantine quadruples in $\{1, \ldots, N\}$ *is*

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

where $C = \dfrac{2^{4/3}}{3\Gamma(2/3)^3} \approx 0.338285.$

This is consistent with Dujella's upper and lower bounds

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

Putting the pieces together

Theorem (M.–Sitar, 2010)

The number of Diophantine quadruples in $\{1, \dots, N\}$ *is*

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

where $C = \dfrac{2^{4/3}}{3\Gamma(2/3)^3} \approx 0.338285$.

This is consistent with Dujella's upper and lower bounds

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

Reducible polynomials

Question 1

When we modified Hooley's argument for the equidistribution of roots of irreducible polynomials, we only considered reducible quadratics since we only needed $x^2 - 1$ for our application.

What about reducible polynomials of degree 3 and greater?

Other than being a perfect power of a linear polynomial, are there any other obstructions that would prevent the roots from being equidistributed?

Reducible polynomials

Question 1

When we modified Hooley's argument for the equidistribution of roots of irreducible polynomials, we only considered reducible quadratics since we only needed $x^2 - 1$ for our application.

What about reducible polynomials of degree 3 and greater?

Other than being a perfect power of a linear polynomial, are there any other obstructions that would prevent the roots from being equidistributed?

Relationship to elliptic curves

Question 2

Can it be shown that there are no Diophantine 5-tuples?

Given a Diophantine quadruple $\{a, b, c, d\}$, we can form the elliptic curves

$$Y^2 = (aX+1)(bX+1)(cX+1)(dX+1)$$

and

$$Y^2 = (X+a)(X+b)(X+c)(X+d).$$

These curves tend to have torsion groups of $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, and moderately large rank. They may (as Dujella noted) lead to information about the conjectured absence of Diophantine 5-tuples.

Relationship to elliptic curves

Question 2

Can it be shown that there are no Diophantine 5-tuples?

Given a Diophantine quadruple $\{a, b, c, d\}$, we can form the elliptic curves

$$Y^2 = (aX + 1)(bX + 1)(cX + 1)(dX + 1)$$

and

$$Y^2 = (X + a)(X + b)(X + c)(X + d).$$

These curves tend to have torsion groups of $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, and moderately large rank. They may (as Dujella noted) lead to information about the conjectured absence of Diophantine 5-tuples.

The end

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