Windmills of the Minds

An Algorithm for Fermat's Two Squares Theorem

Hing Lun Chan

College of Engineering and Computer Science
Australian National University

CPP 2022, 17-18 January 2022.

Outline

1. Sum of Two Squares
2. Windmills
3. Algorithm

Sum of Two Squares

Primes

$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, \ldots$

A **prime** is not 0 or 1, and divisible only by 1 and itself.

Primes

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, \ldots$$

A **prime** is not 0 or 1, and divisible only by 1 and itself.

Even prime: $2 = 1^2 + 1^2$, sum of two squares. Odd primes:

$4k + 1$	$4k + 3$	sum of two squares?

Primes

$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, \ldots$

A **prime** is not 0 or 1, and divisible only by 1 and itself.

Even prime: $2 = 1^2 + 1^2$, sum of two squares. Odd primes:

$4k + 1$ (tik)	$4k + 3$ (tok)	sum of two squares?
	3	
5		$5 = 1^2 + 2^2$
	7	
	11	
13		$13 = 3^2 + 2^2$
17		$17 = 1^2 + 4^2$
	19	

Primes

$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, \ldots$

A **prime** is not 0 or 1, and divisible only by 1 and itself.

Even prime: $2 = 1^2 + 1^2$, sum of two squares. Odd primes:

$4k + 1$ (tik)	$4k + 3$ (tok)	sum of two squares?
	3	
5		$5 = 1^2 + 2^2$
	7	
	11	
13		$13 = 3^2 + 2^2$
17		$17 = 1^2 + 4^2$
	19	
	23	
29		$29 = 5^2 + 2^2$

Primes

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, ...

A **prime** is not 0 or 1, and divisible only by 1 and itself.

Even prime: $2 = 1^2 + 1^2$, sum of two squares. Odd primes:

$4k+1$ (tik)	$4k+3$ (tok)	sum of two squares?
	3	
5		$5 = 1^2 + 2^2$
	7	
	11	
13		$13 = 3^2 + 2^2$
17		$17 = 1^2 + 4^2$
	19	
	23	
29		$29 = 5^2 + 2^2$

If odd n is a sum of two squares, n = odd square + even square.

Two Squares Theorem

A tik prime is a sum of two squares, odd and even, uniquely.

$$\vdash \text{prime } n \Rightarrow (n \equiv 1 \pmod 4 \iff \exists!(u,v).\ \text{odd } u \wedge \text{even } v \wedge n = u^2 + v^2)$$

Two Squares Theorem

A tik prime is a sum of two squares, odd and even, uniquely.

$\vdash \text{prime } n \Rightarrow (n \equiv 1 \pmod 4 \iff \exists!(u,v).\ \text{odd } u \wedge \text{even } v \wedge n = u^2 + v^2)$

- 1640 Fermat's X'mas letter, claimed he had an "irrefutable" proof.
- 1659 Fermat's letter, hinted a proof by "infinite descent", very rare!

Two Squares Theorem

A tik prime is a sum of two squares, odd and even, uniquely.

$$\vdash \text{prime } n \Rightarrow (n \equiv 1 \pmod 4 \iff \exists!(u,v).\ \text{odd } u \wedge \text{even } v \wedge n = u^2 + v^2)$$

- 1640 Fermat's X'mas letter, claimed he had an "irrefutable" proof.
- 1659 Fermat's letter, hinted a proof by "infinite descent", very rare!
- 1749 Euler proved by infinite descent, worked "on & off for 7 years".
- 1775 Lagrange proved by creating a theory of quadratic forms.
- 1801 Gauss revised Lagrange's proof, invented Gaussian integers.

Two Squares Theorem

A tik prime is a sum of two squares, odd and even, uniquely.

$$\vdash \text{prime } n \Rightarrow (n \equiv 1 \pmod 4 \iff \exists!(u,v).\ \text{odd } u \wedge \text{even } v \wedge n = u^2 + v^2)$$

- 1640 Fermat's X'mas letter, claimed he had an "irrefutable" proof.
- 1659 Fermat's letter, hinted a proof by "infinite descent", very rare!
- 1749 Euler proved by infinite descent, worked "on & off for 7 years".
- 1775 Lagrange proved by creating a theory of quadratic forms.
- 1801 Gauss revised Lagrange's proof, invented Gaussian integers.
- 1877, 1894 Dedekind offered 2 proofs, based on Gaussian integers.
- Many other proofs, based on:
  - Jacobi sums,
  - Pigeonhole principle,
  - Continued fractions,
  - ...

Windmills and Minds

Tik Shapes

A tik (✓) number $n = 4k + 1$ for some k.
A picture for $n = 37$.

Tik Shapes

A tik (✓) number $n = 4k + 1$ for some k.
A picture for $n = 37$.

$$\begin{aligned} 37 &= 1 &&+ 4(9) \\ &= (1 \times 1) &&+ 4(9 \times 1) \end{aligned}$$

Tik Shapes

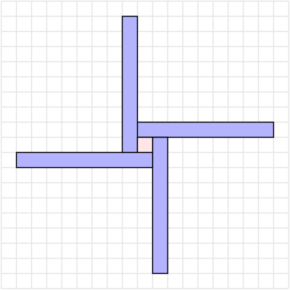
A tik (✓) number $n = 4k + 1 \quad$ for some k.
A picture for $n = 37$.

$$\begin{aligned} 37 &= 1 &&+ 4(9) \\ &= \overbrace{(1 \times 1)}^{\text{a square}} &&+ \overbrace{4(9 \times 1)}^{\text{4 rectangles}} \end{aligned}$$

Tik Shapes

A tik (✓) number $n = 4k + 1$ for some k.
A picture for $n = 37$.

$$\begin{aligned} 37 &= 1 && + \; 4(9) \\ &= \underbrace{(1 \times 1)}_{\text{a square}} && + \; \underbrace{4(9 \times 1)}_{\text{4 rectangles}} \end{aligned}$$

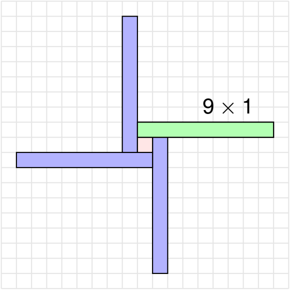


A windmill!

Tik Shapes

A tik (✓) number $n = 4k + 1$ for some k.
A picture for $n = 37$.

$$\begin{aligned} 37 &= 1 &&+ 4(9) \\ &= \underbrace{(1 \times 1)}_{\text{a square}} &&+ \underbrace{4(9 \times 1)}_{\text{4 rectangles}} \end{aligned}$$



A windmill!

Tik Shapes (continued)

Another picture for $n = 37$.

Tik Shapes (continued)

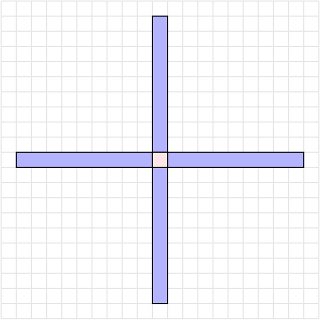
Another picture for $n = 37$.

$$\begin{aligned} 37 &= 1 && + && 4(9) \\ &= \overbrace{(1 \times 1)}^{\text{a square}} && + && \overbrace{4(1 \times 9)}^{\text{4 rectangles}} \end{aligned}$$

Tik Shapes (continued)

Another picture for $n = 37$.

$$\begin{aligned} 37 &= 1 && + \quad 4(9) \\ &= \overbrace{(1 \times 1)}^{\text{a square}} && + \quad \overbrace{4(1 \times 9)}^{\text{4 rectangles}} \end{aligned}$$

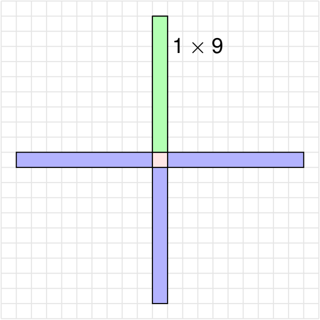


Another windmill!

Tik Shapes (continued)

Another picture for $n = 37$.

$$\begin{aligned} 37 &= \quad 1 & &+ \quad 4(9) \\ &= \quad \overbrace{(1 \times 1)}^{\text{a square}} & &+ \quad \overbrace{4(1 \times 9)}^{\text{4 rectangles}} \end{aligned}$$

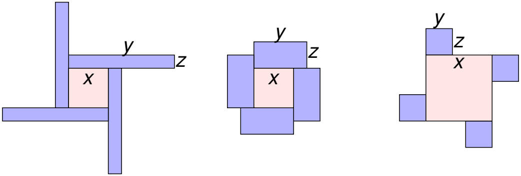


Another windmill!

Windmill

windmill: a central square with four identical rectangular arms.

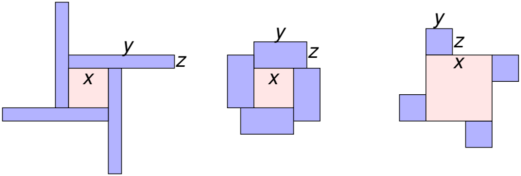
windmill $x\ y\ z \stackrel{\text{def}}{=} x^2 + 4yz$



Windmill

windmill: a central square with four identical rectangular arms.

windmill $x\ y\ z \stackrel{\text{def}}{=} x^2 + 4yz$

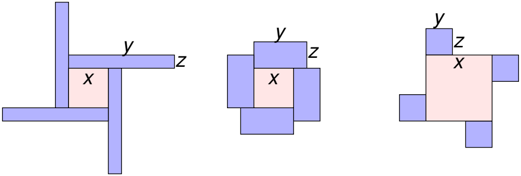


- Denote (windmill $x\ y\ z$) by a triple (x, y, z).
- Value x is the size (or side) of the central square.
- Values y, z are the length and width of *top* arm of central square.
- The 4 arms are arranged clockwise around the central square.

Windmill

windmill: a central square with four identical rectangular arms.

windmill $x\ y\ z \stackrel{\text{def}}{=} x^2 + 4yz$



- Denote (windmill $x\ y\ z$) by a triple (x, y, z).
- Value x is the size (or side) of the central square.
- Values y, z are the length and width of *top* arm of central square.
- The 4 arms are arranged clockwise around the central square.
- Every ✓ number has at least one windmill.

Mills

How many windmills for $n = 37$?

Mills

How many windmills for $n = 37$?

- recall $n = x^2 + 4yz$, with x odd.
- compute $n - x^2 = 4yz$, for all odd x.

Mills

How many windmills for $n = 37$?

- recall $n = x^2 + 4yz$, with x odd.
- compute $n - x^2 = 4yz$, for all odd x.

odd x	$n - x^2$	$=$	$4yz$	triple (x, y, z)
1	$37 - 1^2$	$=$	$36 = 4(9)$	$(1, 1, 9), (1, 9, 1), (1, 3, 3)$
3	$37 - 3^2$	$=$	$28 = 4(7)$	$(3, 1, 7), (3, 7, 1)$
5	$37 - 5^2$	$=$	$12 = 4(3)$	$(5, 1, 3), (5, 3, 1)$
7	$37 - 7^2$	$=$	negative!	

Mills

How many windmills for $n = 37$?

- recall $n = x^2 + 4yz$, with x odd.
- compute $n - x^2 = 4yz$, for all odd x.

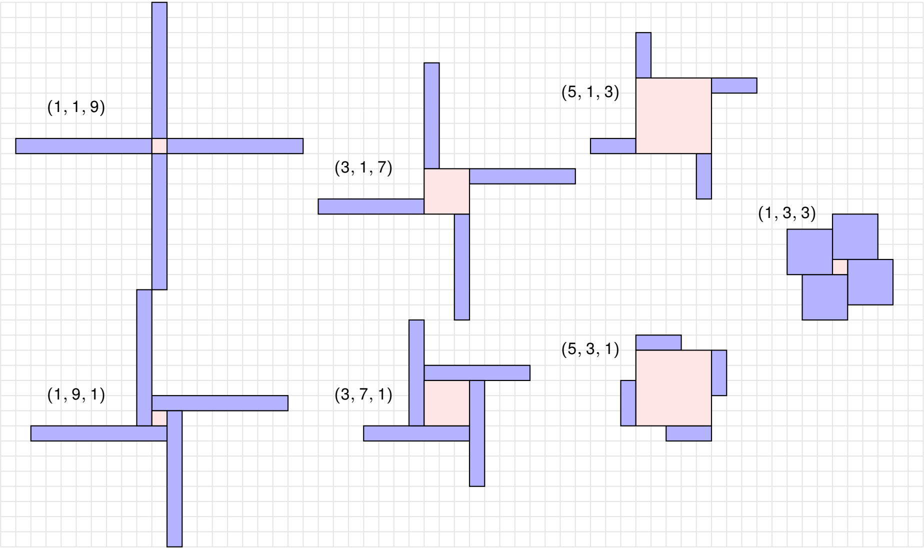
odd x	$n - x^2$	=	$4yz$	triple (x, y, z)
1	$37 - 1^2$	=	$36 = 4(9)$	$(1, 1, 9), (1, 9, 1), (1, 3, 3)$
3	$37 - 3^2$	=	$28 = 4(7)$	$(3, 1, 7), (3, 7, 1)$
5	$37 - 5^2$	=	$12 = 4(3)$	$(5, 1, 3), (5, 3, 1)$
7	$37 - 7^2$	=	negative!	

All the windmills of a ✓ number form its **mills.** Thus,

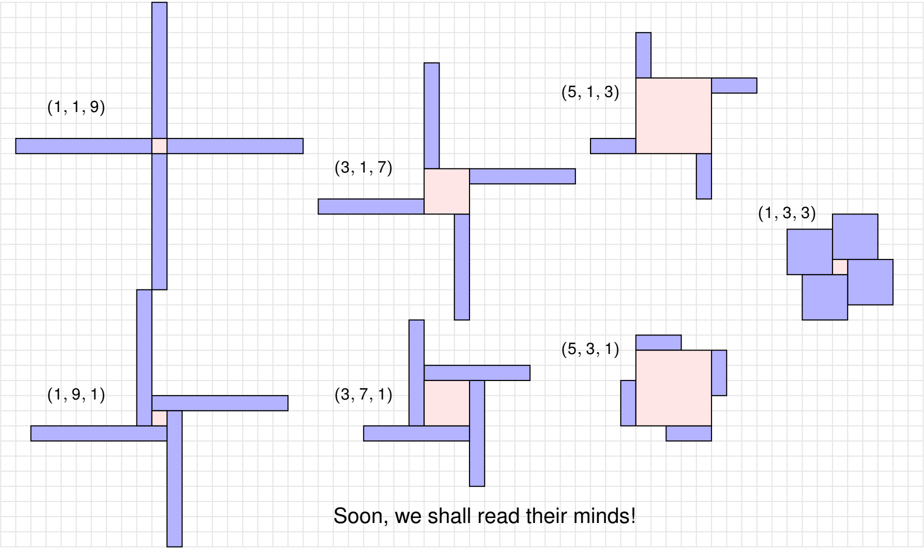
$$\text{mills } 37 = \{(1, 1, 9), (1, 9, 1), (1, 3, 3), (3, 1, 7), (3, 7, 1), (5, 1, 3), (5, 3, 1)\}$$

How many windmills? $|\text{mills } 37| = 7$, an odd number.

Windmills of $n = 37$

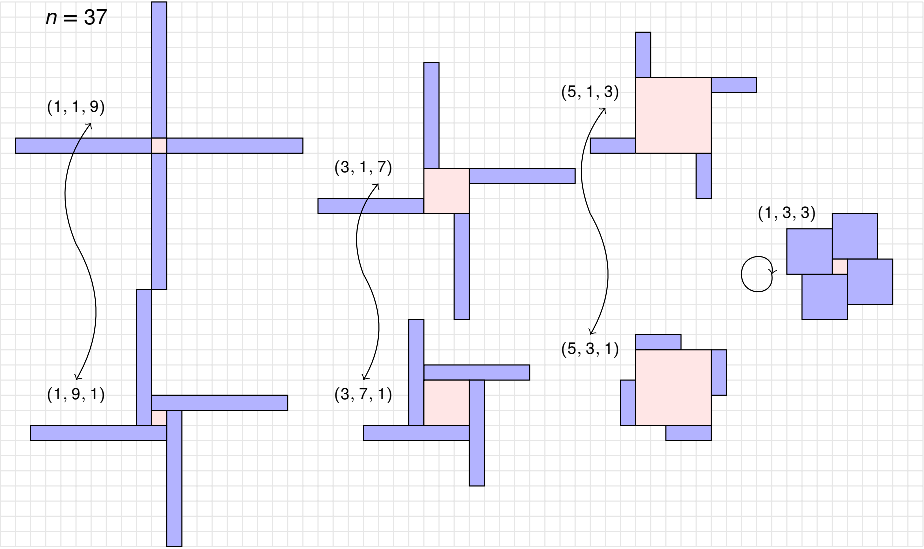


Windmills of $n = 37$

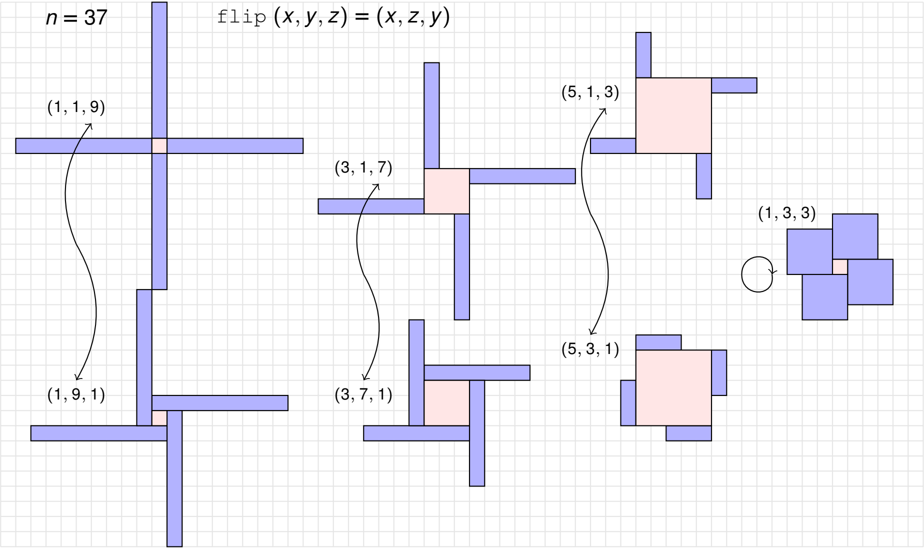


Soon, we shall read their minds!

Windmills related by Flips

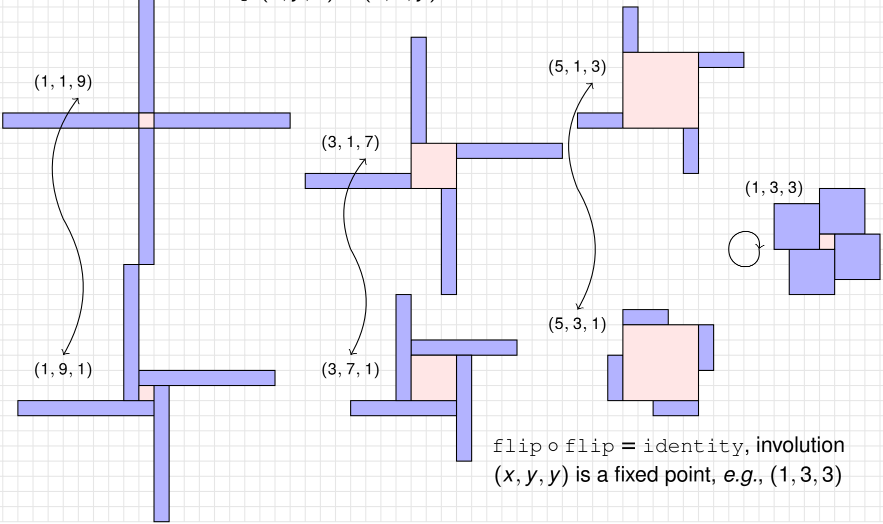


Windmills related by Flips



Windmills related by Flips

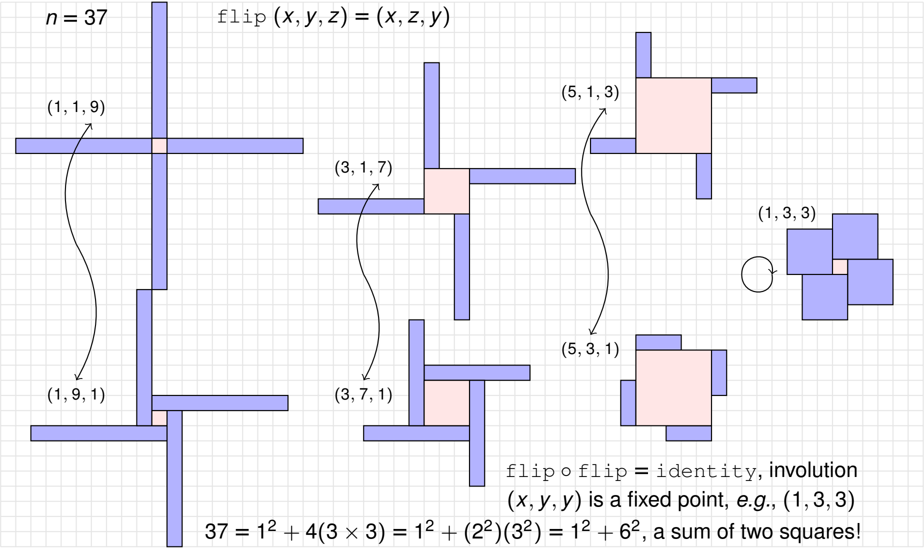
$n = 37$ `flip` $(x, y, z) = (x, z, y)$



`flip` $\circ$ `flip` = `identity`, involution

(x, y, y) is a fixed point, *e.g.*, $(1, 3, 3)$

Windmills related by Flips



flip ∘ flip = identity, involution

(x, y, y) is a fixed point, *e.g.*, $(1, 3, 3)$

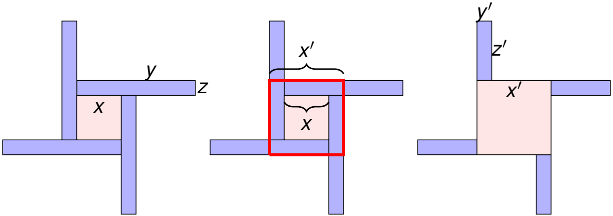
$37 = 1^2 + 4(3 \times 3) = 1^2 + (2^2)(3^2) = 1^2 + 6^2$, a sum of two squares!

Mind

The **mind** of a windmill: biggest (square) heart of the overall shape.

Mind

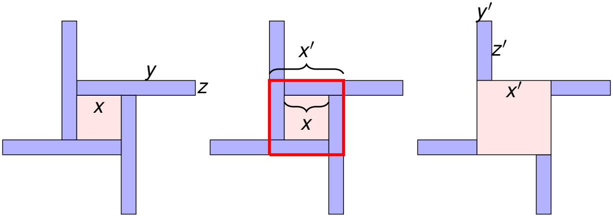
The **mind** of a windmill: biggest (square) heart of the overall shape.



A windmill transforms to another windmill through the mind (in red).

Mind

The **mind** of a windmill: biggest (square) heart of the overall shape.

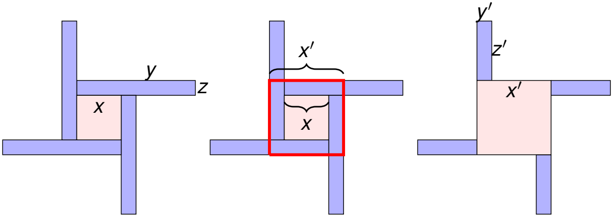


A windmill transforms to another windmill through the mind (in red).

- (left to right) expand central square through mind, shrinking arms.
- (right to left) shrink central square through mind, expanding arms.

Mind

The **mind** of a windmill: biggest (square) heart of the overall shape.



A windmill transforms to another windmill through the mind (in red).

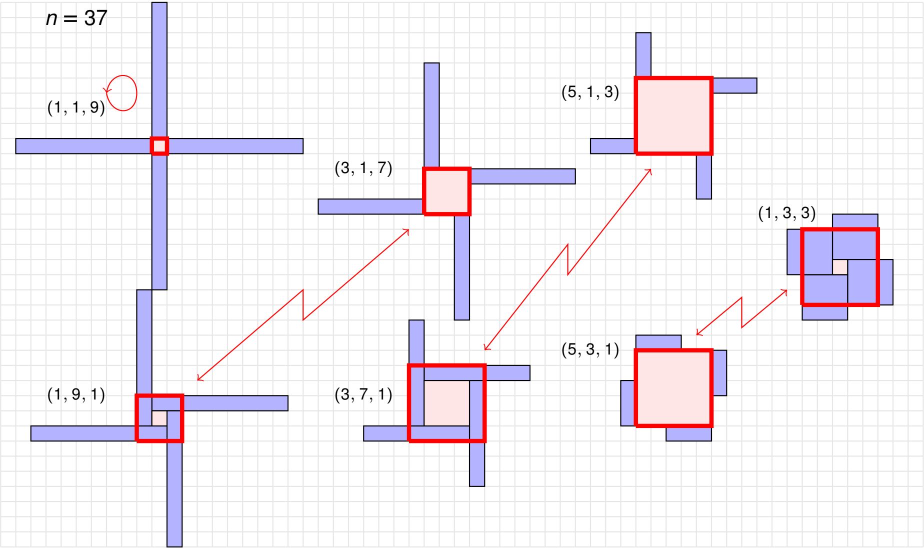
- (left to right) expand central square through mind, shrinking arms.
- (right to left) shrink central square through mind, expanding arms.

$$\mathtt{mind}\,(x, y, z) = \text{length of square mind}$$

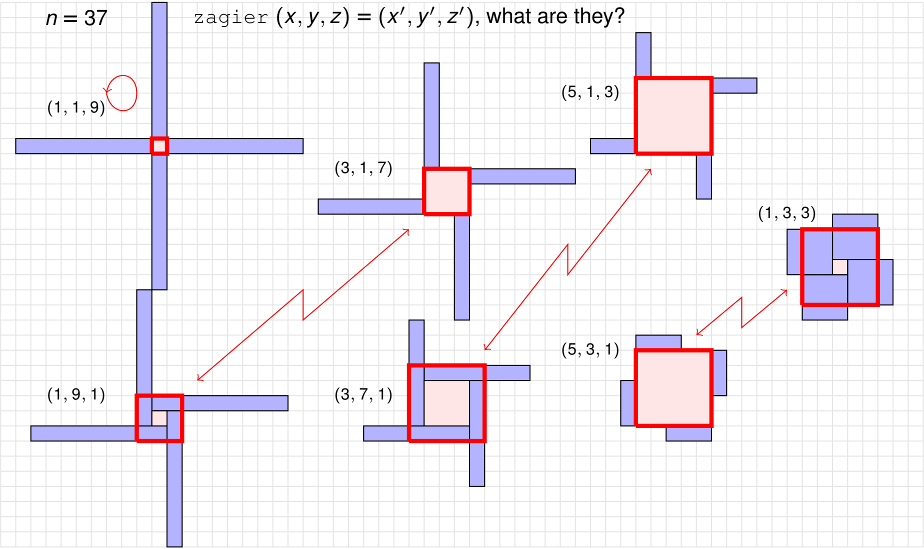
Using simple geometry,

$$\mathtt{mind}\,(x, y, z) = \begin{cases} x + 2z & \text{if } x < y - z \\ 2y - x & \text{else if } x < y \\ x & \text{otherwise} \end{cases}$$

Windmills related by Minds

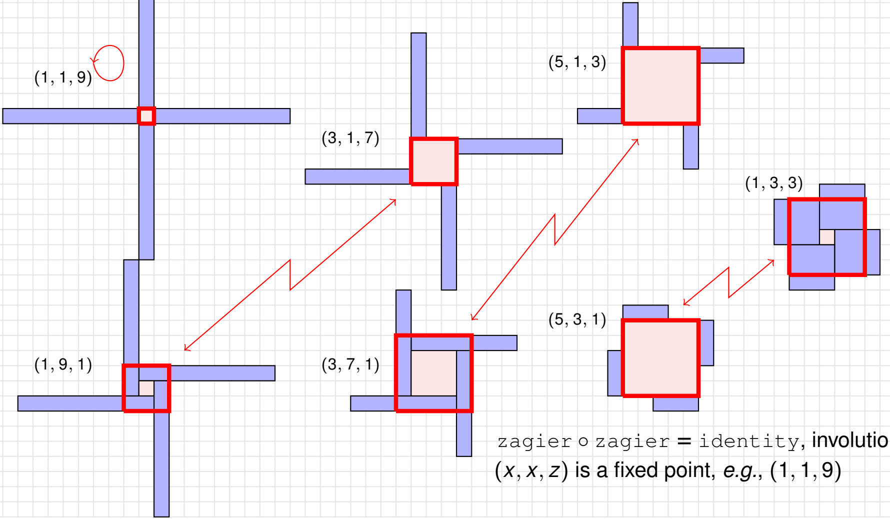


Windmills related by Minds



Windmills related by Minds

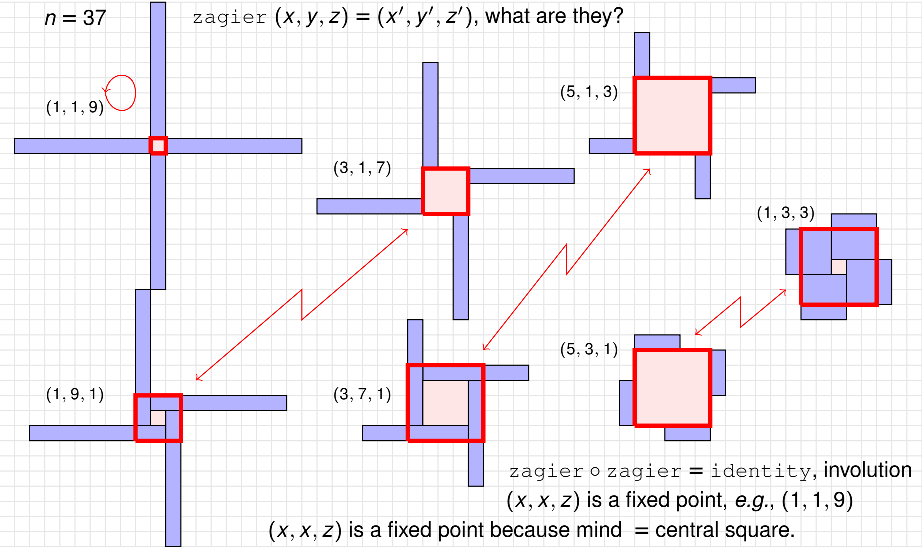
$n = 37$ `zagier` $(x, y, z) = (x', y', z')$, what are they?



`zagier` $\circ$ `zagier` = `identity`, involution

(x, x, z) is a fixed point, *e.g.*, $(1, 1, 9)$

Windmills related by Minds



zagier $\circ$ zagier = identity, involution

(x, x, z) is a fixed point, *e.g.*, $(1, 1, 9)$

(x, x, z) is a fixed point because mind = central square.

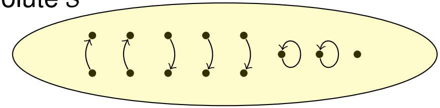
Involution

A map f that can undo itself is an **involution**: $f \circ f = \texttt{identity}$.

Involution

A map f that can undo itself is an **involution**: $f \circ f = \texttt{identity}$.

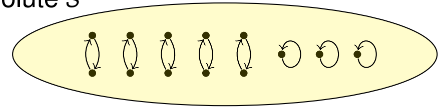
f involute S



Involution

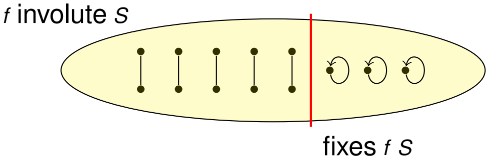
A map f that can undo itself is an **involution**: $f \circ f = \texttt{identity}$.

f involute S



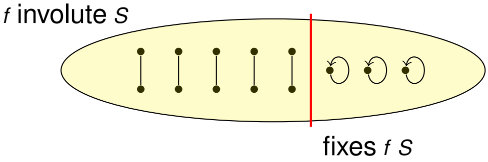
Involution

A map f that can undo itself is an **involution**: $f \circ f = \texttt{identity}$.



Involution

A map f that can undo itself is an **involution**: $f \circ f = \texttt{identity}$.



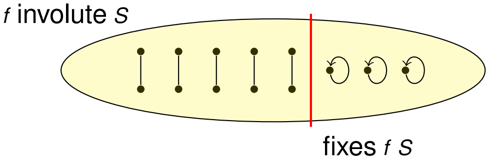
For an involution f on a finite set S, due to pairing:

Theorem

$\vdash$finite $S \wedge f$ involute $S \Rightarrow$ (odd $|S| \iff$ odd $|$fixes f $S|$)

Involution

A map f that can undo itself is an **involution**: $f \circ f = \texttt{identity}$.



For an involution f on a finite set S, due to pairing:

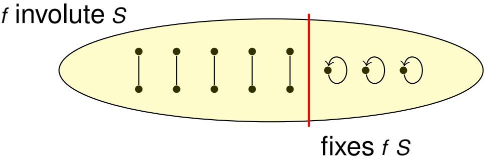
Theorem

$\vdash$finite $S \wedge f$ involute $S \Rightarrow$ (odd $|S| \iff$ odd $|$fixes f $S|$)

- For any involution, *only one* fixed point $\Rightarrow$ size of set is *odd*.
- For any involution, size of set is *odd* $\Rightarrow$ *at least one* fixed point.

Involution

A map f that can undo itself is an **involution**: $f \circ f = \texttt{identity}$.



For an involution f on a finite set S, due to pairing:

Theorem

$\vdash$finite $S \wedge f$ involute $S \Rightarrow$ (odd $|S| \iff$ odd $|$fixes f $S|$)

- For any involution, *only one* fixed point $\Rightarrow$ size of set is *odd*.
- For any involution, size of set is *odd* $\Rightarrow$ *at least one* fixed point.
- Given a ✓prime $n = 4k + 1$, `zagier` fix is $(1, 1, k)$ only.
- So $|$mills $n|$ is **odd**, `flip` fix exists, n is a sum of two squares!

Zagier's Proof

A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares

D. ZAGIER
Department of Mathematics, University of Maryland, College Park, MD 20742

The involution on the finite set $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ defined by

$$(x, y, z) \mapsto \begin{cases} (x + 2z,\ z,\ y - x - z) & \text{if } x < y - z \\ (2y - x,\ y,\ x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y,\ x - y + z,\ y) & \text{if } x > 2y \end{cases}$$

has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x, y, z) \mapsto (x, z, y)$ also has a fixed point. □

Don Zagier's famous proof of Fermat's Two Squares Theorem, February 1990.

Zagier's Proof

A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares

D. Zagier
Department of Mathematics, University of Maryland, College Park, MD 20742

The involution on the finite set $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ defined by

$$(x,y,z) \mapsto \begin{cases} (x + 2z,\ z,\ y - x - z) & \text{if } x < y - z \\ (2y - x,\ y,\ x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y,\ x - y + z,\ y) & \text{if } x > 2y \end{cases}$$

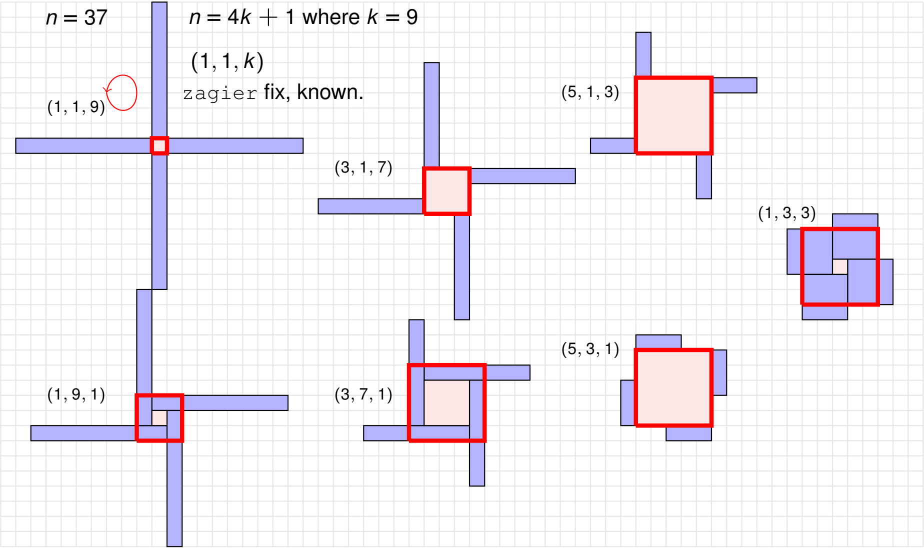
has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x,y,z) \mapsto (x,z,y)$ also has a fixed point. □

Don Zagier's famous proof of Fermat's Two Squares Theorem, February 1990.

All these have been formalised in other theorem provers!

Two Squares Algorithm

Two Squares Algorithm



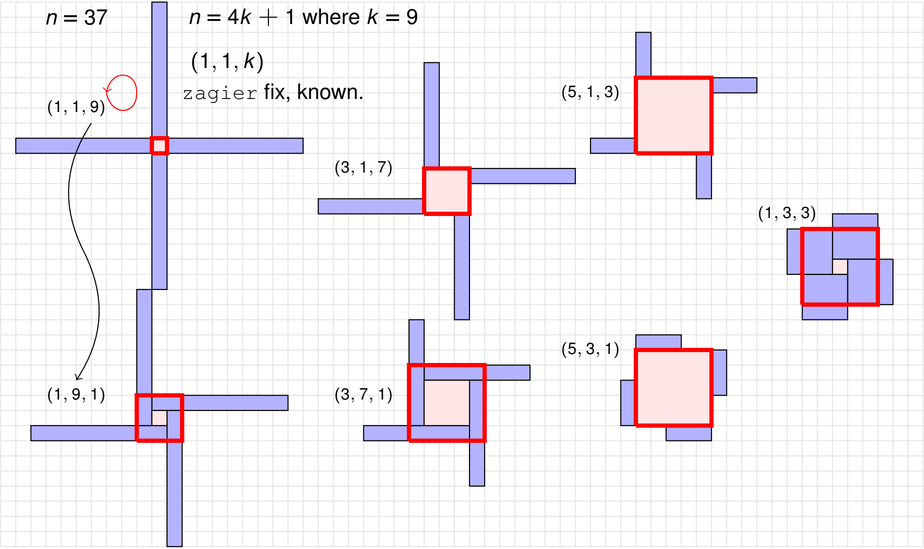
Two Squares Algorithm

$n = 37$

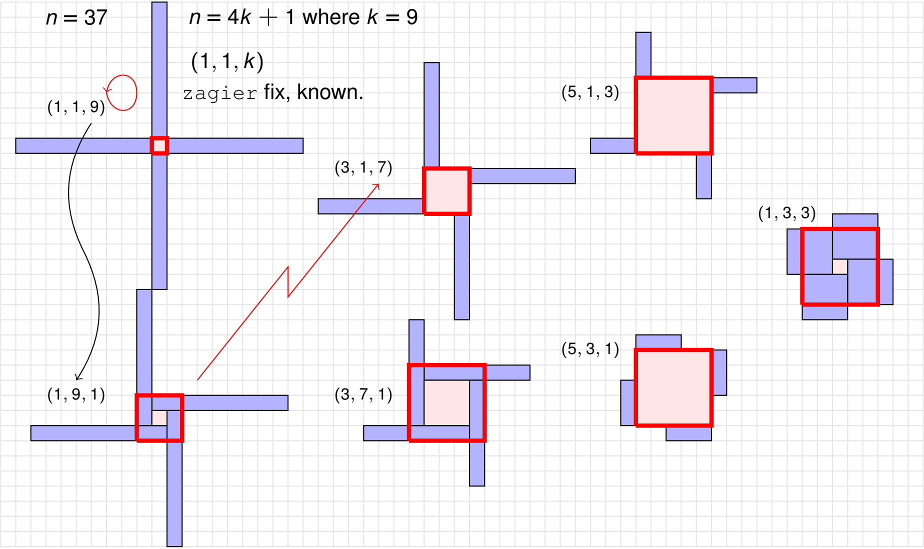
$n = 4k + 1$ where $k = 9$

$(1, 1, k)$

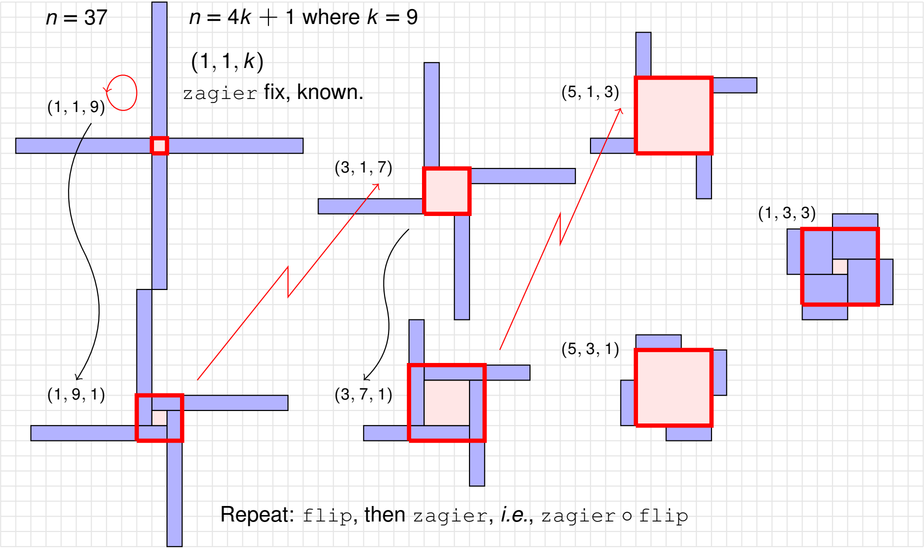
`zagier` fix, known.



Two Squares Algorithm

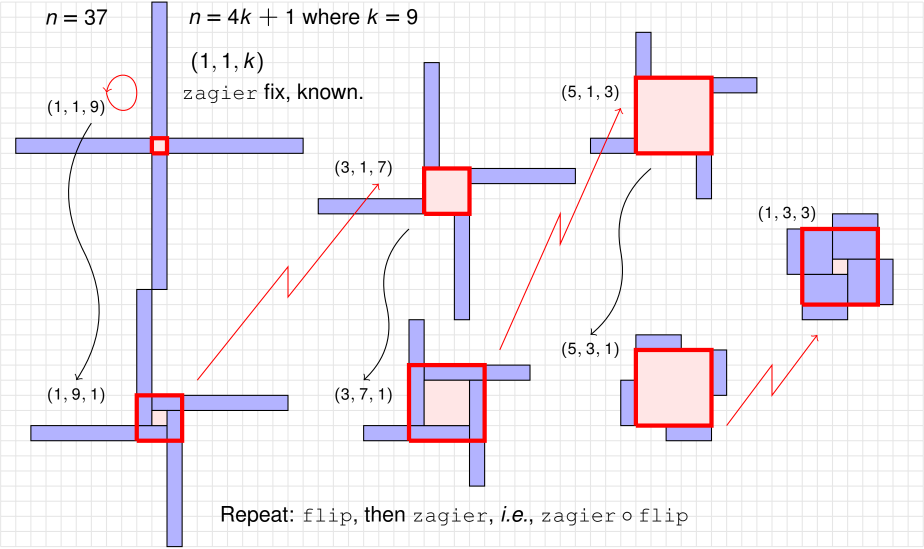


Two Squares Algorithm



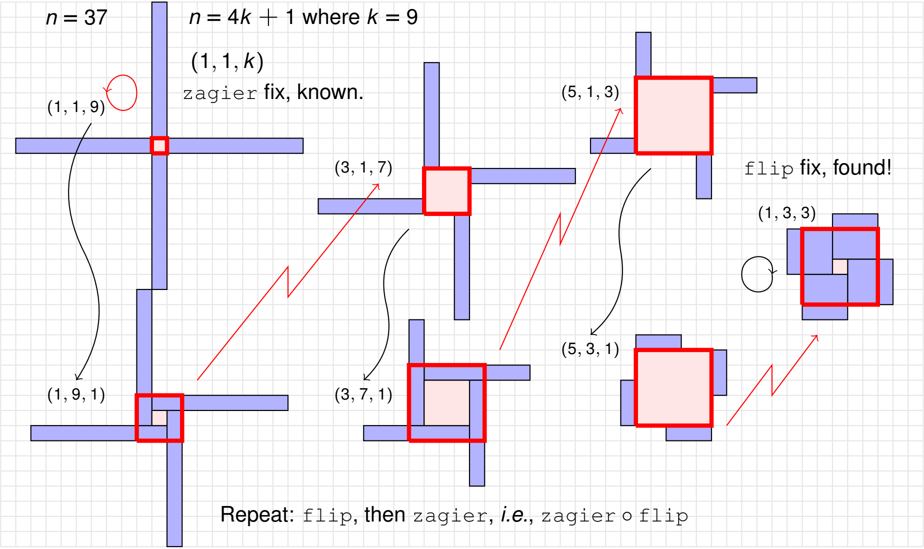
Repeat: `flip`, then `zagier`, *i.e.*, `zagier` $\circ$ `flip`

Two Squares Algorithm



Repeat: `flip`, then `zagier`, *i.e.*, `zagier` ∘ `flip`

Two Squares Algorithm



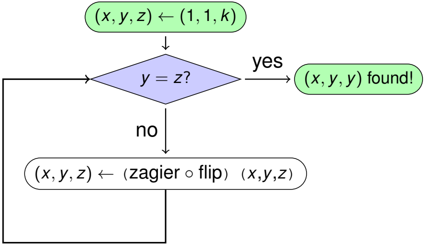
Repeat: `flip`, then `zagier`, *i.e.*, `zagier` ∘ `flip`

Algorithm Code

- *Input*: a tik (✓) number $n = 4k + 1$.
- *Output*: a flip fix triple (x, y, y) so that $n = x^2 + (2y)^2$.

Algorithm Code

- *Input*: a tik (✓) number $n = 4k + 1$.
- *Output*: a flip fix triple (x, y, y) so that $n = x^2 + (2y)^2$.

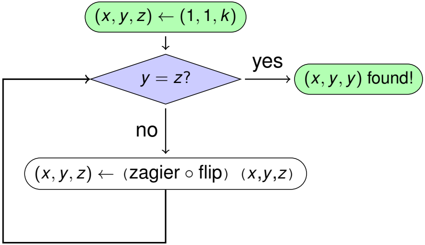


Method: use a triple t.

- start with $t = (1,1,k)$, the `zagier` fix.
- while (t is not of the form (x, y, y)) :
- $t \leftarrow$ `flip` t
- $t \leftarrow$ `zagier` t
- end while.
- return t, which is a `flip` fix.

Algorithm Code

- *Input*: a tik (✓) number $n = 4k + 1$.
- *Output*: a flip fix triple (x, y, y) so that $n = x^2 + (2y)^2$.



Method: use a triple t.

- start with $t = (1,1,k)$, the `zagier` fix.
- while (t is not of the form (x, y, y)) :
- $t \leftarrow$ `flip` t
- $t \leftarrow$ `zagier` t
- end while.
- return t, which is a `flip` fix.

- `flip` is just swapping y, z of triple.
- `zagier` has double, add and subtract only.
- Algorithm is simple, and fast for ✓ primes n not-too-large.
- Need to prove: code is correct, and will terminate for a ✓ prime.

Algorithm Run

Executing the algorithm in HOL4 for ✓ prime $n = 37$:

```
> EVAL ``two_squares 37``;
val it = |- two_squares 37 = (1,6): thm
```

HOL4 allows timing of an execution:

```
> time EVAL ``two_squares 37``;
runtime: 0.00379s,    gctime: 0.00000s,     systime: 0.00928s.
val it = |- two_squares 37 = (1,6): thm
```

Algorithm Run

Executing the algorithm in HOL4 for ✓ prime $n = 37$:

```
> EVAL ‘‘two_squares 37‘‘;
val it = |- two_squares 37 = (1,6): thm
```

HOL4 allows timing of an execution:

```
> time EVAL ‘‘two_squares 37‘‘;
runtime: 0.00379s,    gctime: 0.00000s,     systime: 0.00928s.
val it = |- two_squares 37 = (1,6): thm
```

More examples:

```
> time EVAL ‘‘two_squares 97‘‘;
runtime: 0.00770s, gctime: 0.00086s, systime: 0.00077s.
val it = |- two_squares 97 = (9,4): thm
> time EVAL ‘‘two_squares 1999999913‘‘;
runtime: 2m23s, gctime: 14.7s, systime: 11.3s.
val it = |- two_squares 1999999913 = (1093,44708): thm
> time EVAL ‘‘two_squares 12345678949‘‘;
runtime: 6m02s,    gctime: 37.5s,     systime: 26.0s.
val it = |- two_squares 12345678949 = (110415,12418): thm
```

Algorithm Correctness

Preprint of paper at arXiv: `https://arxiv.org/abs/2112.02556`

Windmills of the Minds: An Algorithm for Fermat's Two Squares Theorem

Hing Lun Chan
Australian National University
Canberra, Australia
joseph.chan@anu.edu.au

Abstract

The two squares theorem of Fermat is a gem in number theory, with a spectacular one-sentence "proof from the Book". Here is a formalisation of this proof, with an interpretation using windmill patterns. The theory behind involves involutions on a finite set, especially the parity of the number of fixed points in the involutions. Starting as an existence proof that is non-constructive, there is an ingenious way to turn it into a constructive one. This gives an algorithm to compute the two squares by iterating the two involutions alternatively from a known fixed point.

CCS Concepts: • **Theory of computation → Automated reasoning**;

Keywords: Number Theory, Algorithm, Iteractive Theorem Proving.

The involution on the finite set

$$S = \{(x, y, z) \in \mathbb{N}^3 \mid n = x^2 + 4yz\}$$

defined by

$$(x,y,z) \longmapsto \begin{cases} (x + 2z, z, y - z - x) & \text{if } x < y - z \\ (2y - x, y, x + z - y) & \text{if } y - z < x < 2y \\ (x - 2y, x + z - y, y) & \text{if } x > 2y \end{cases} \quad (1)$$

has exactly one fixed point, so $|S|$ is odd, and the involution defined by $(x,y,z) \longmapsto (x,z,y)$ also has a fixed point.

Algorithm Correctness

Preprint of paper at arXiv: `https://arxiv.org/abs/2112.02556`

Windmills of the Minds: An Algorithm for Fermat's Two Squares Theorem

Hing Lun Chan
Australian National University
Canberra, Australia
joseph.chan@anu.edu.au

Abstrac

The two s
ory, with
Here is a f
using win
lutions or
of fixed p
proof that
turn it int
compute t
alternativ

CCS Con
reasonin

Keywords
Proving.

$< 2y$ (1)

d the
has a

Permutation by involution ∘ involution.

Permutation orbits and periods.

Algorithm Correctness

Preprint of paper at arXiv: `https://arxiv.org/abs/2112.02556`

Windmills of the Minds: An Algorithm for Fermat's Two Squares Theorem

Hing Lun Chan
Australian National University
Canberra, Australia
joseph.chan@anu.edu.au

Abstrac

The two s
ory, with
Here is a f
using win
lutions on
of fixed p
proof that
turn it int
compute t
alternativ

< 2y (1)

CCS Conc
reasonin

d the
has a

Keywords
Proving.

Permutation by involution ∘ involution.

Permutation orbits and periods.

Orbits connecting fixed points.

Orbits with odd or even periods.

Thank you!