Fun With Pythagorean Triples

Allan Bickle

Dordt College

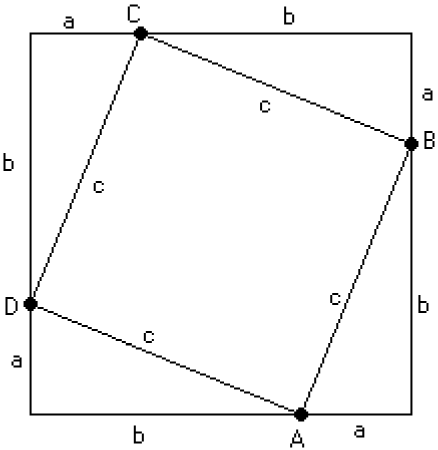
October 25, 2013

The Pythagorean Theorem is a basic fact about geometry.

Theorem

[Pythagorean Theorem] If a right triangle has legs with lengths a and b and hypotenuse with length c, then $a^2 + b^2 = c^2$.

The Pythagorean Theorem



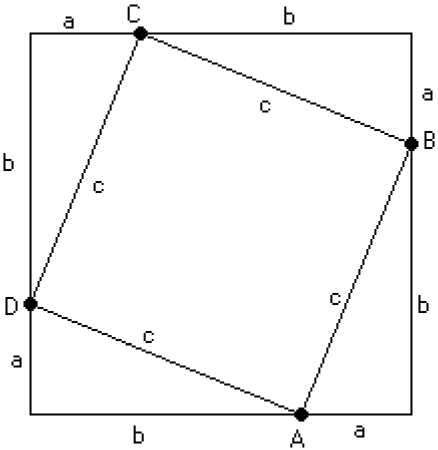
Compute the area two ways.

$(a+b)^2 = 4\left(\frac{1}{2}ab\right) + c^2$

$a^2 + 2ab + b^2 = 2ab + c^2$

$a^2 + b^2 = c^2$

The Pythagorean Theorem



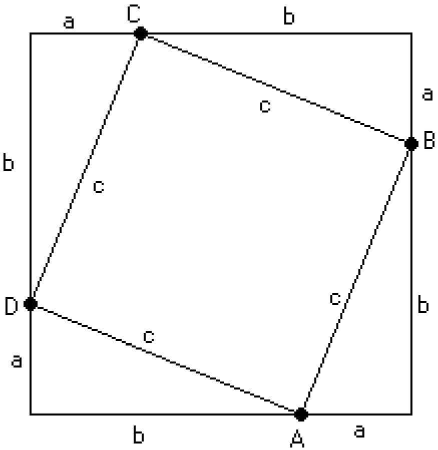
Compute the area two ways.

$(a+b)^2 = 4\left(\frac{1}{2}ab\right) + c^2$

$a^2 + 2ab + b^2 = 2ab + c^2$

$a^2 + b^2 = c^2$

The Pythagorean Theorem

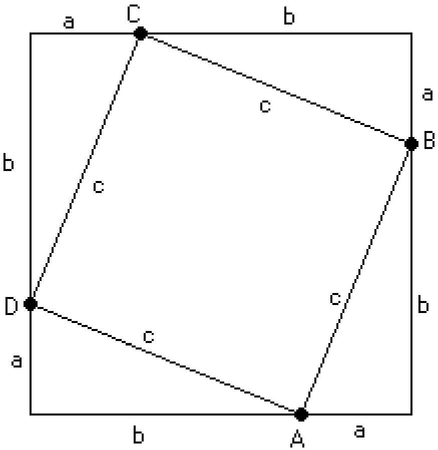


Compute the area two ways.

$(a+b)^2 = 4\left(\frac{1}{2}ab\right) + c^2$

$a^2 + 2ab + b^2 = 2ab + c^2$

$a^2 + b^2 = c^2$



Compute the area two ways.

$(a+b)^2 = 4\left(\frac{1}{2}ab\right) + c^2$

$a^2 + 2ab + b^2 = 2ab + c^2$

$a^2 + b^2 = c^2$

The Pythagorean Theorem

- There are many proofs of the Pythagorean Theorem.
- One book contains 370 proofs-perhaps the most for any theorem.
- (This raises the question of when two proofs should be considered distinct.)
- It is possible for the numbers a, b, and c to all be integers.
- Example: $3^2 + 4^2 = 5^2$

Definition

A triple of integers (a, b, c) with $a^2 + b^2 = c^2$ is called a Pythagorean Triple.

History

- The Pythagorean Theorem is named for Pythagoras, in ancient Greece.
- Methods for generating such triples have been studied in many cultures, beginning with the Babylonians.
- They were later studied by the ancient Greek, Chinese, and Indian mathematicians.
- An application of Pythagorean triples is in homework problems where the author wants the calculations to work out simply.

Trivial Cases

- There are some trivial cases
- We see $(0, b, b)$ is a Pythagorean triple, since $0^2 + b^2 = b^2$.
- If $a^2 + b^2 = c^2$, then $(\pm a)^2 + (\pm b)^2 = (\pm c)^2$.
- Hence we typically require that a,b, and c be positive integers.
- If $a^2 + b^2 = c^2$, then $(ka)^2 + (kb)^2 = (kc)^2$, so (ka, kb, kc) is a Pythagorean triple.
- Thus if a, b, and c have a common factor, it can be divided out to obtain a smaller Pythagorean triple.

Definition

A Pythagorean triple where a, b, and c have no common factor is called a primitive Pythagorean triple.

- The most famous Pythagorean triple is $(3, 4, 5)$.
- The next most famous Pythagorean triple is $(5, 12, 13)$.
- Another common Pythagorean triple is $(7, 24, 25)$.
- Do you see a pattern?

Finding a Pattern

- Start with an odd positive integer.
- Square it, and divide the square into two integers that differ by one.
- This produces a Pythagorean triple.
- Algebraically, for $n = 2k + 1$,

$$\left(n, \frac{n^2 - 1}{2}, \frac{n^2 + 1}{2}\right)$$

  is a Pythagorean triple. This is easily verified.
- Thus $(9, 40, 41)$, $(11, 60, 61)$, $(13, 84, 85)$, $(15, 112, 113)$, $(17, 144, 145)$, ... are Pythagorean triples.
- I first discovered this pattern (without proof) as a middle-grade student.
- However, not all Pythagorean triples satisfy this pattern!
- Example: $(8, 15, 17)$.

A General Solution

- Can we find a general solution that produces all primitive Pythagorean triples?
- A few observations:
- a and b cannot both be even, since then c would be even also.
- An even square equals 0 (mod 4), since $(2k)^2 = 4k^2$.
- An odd square equals 1 (mod 4), since $(2k+1)^2 = 4k^2 + 4k + 1$.
- a and b cannot both be odd, since then c would equal 2 (mod 4).
- Thus let a be even and b be odd, so c must be odd.

A General Solution

Try some algebra.

$$a^2 + b^2 = c^2$$

$$b^2 = c^2 - a^2$$

$$b^2 = (c + a)(c - a)$$

$$\frac{c + a}{b} = \frac{b}{c - a}$$

A General Solution

Try some algebra.

$$a^2 + b^2 = c^2$$

$$b^2 = c^2 - a^2$$

$$b^2 = (c + a)(c - a)$$

$$\frac{c + a}{b} = \frac{b}{c - a}$$

A General Solution

Let $\frac{c+a}{b} = \frac{m}{n}$ (reduced). Then $\frac{c-a}{b} = \frac{n}{m}$.

Adding, we find

$$2\frac{c}{b} = \frac{m}{n} + \frac{n}{m} = \frac{m^2+n^2}{mn}$$

so

$$\frac{c}{b} = \frac{m^2+n^2}{2mn}$$

Similarly, subtracting yields

$$\frac{a}{b} = \frac{m^2-n^2}{2mn}$$

We would like to equate numerators and denominators. Since the left sides are reduced, we need the right sides reduced. Thus we need m and n to have opposite parity. Note also that if m and m^2+n^2 had a common factor, then so would m and n. The other cases are similar.

A General Solution

Let $\frac{c+a}{b} = \frac{m}{n}$ (reduced). Then $\frac{c-a}{b} = \frac{n}{m}$.
Adding, we find

$$2\frac{c}{b} = \frac{m}{n} + \frac{n}{m} = \frac{m^2+n^2}{mn}$$

so

$$\frac{c}{b} = \frac{m^2+n^2}{2mn}$$

Similarly, subtracting yields

$$\frac{a}{b} = \frac{m^2-n^2}{2mn}$$

We would like to equate numerators and denominators. Since the left sides are reduced, we need the right sides reduced. Thus we need m and n to have opposite parity. Note also that if m and m^2+n^2 had a common factor, then so would m and n. The other cases are similar.

A General Solution

Let $\frac{c+a}{b} = \frac{m}{n}$ (reduced). Then $\frac{c-a}{b} = \frac{n}{m}$.
Adding, we find

$$2\frac{c}{b} = \frac{m}{n} + \frac{n}{m} = \frac{m^2+n^2}{mn}$$

so

$$\frac{c}{b} = \frac{m^2+n^2}{2mn}$$

Similarly, subtracting yields

$$\frac{a}{b} = \frac{m^2-n^2}{2mn}$$

We would like to equate numerators and denominators. Since the left sides are reduced, we need the right sides reduced. Thus we need m and n to have opposite parity. Note also that if m and m^2+n^2 had a common factor, then so would m and n. The other cases are similar.

Putting this all together, we have

Theorem

All primitive Pythagorean triples (a, b, c) *with* $a^2 + b^2 = c^2$ *are given by*

$$\begin{aligned} a &= m^2 - n^2 \\ b &= 2mn \\ c &= m^2 + n^2 \end{aligned}$$

where $m > n > 0$, *m and n are relatively prime, and m and n have opposite parity.*

It is easy to check that this gives a Pythagorean triple, as

$$a^2 + b^2 = \left(m^2 - n^2\right)^2 + (2mn)^2 = \left(m^2 + n^2\right)^2 = c^2$$

Pythagorean Triples with Small Lengths

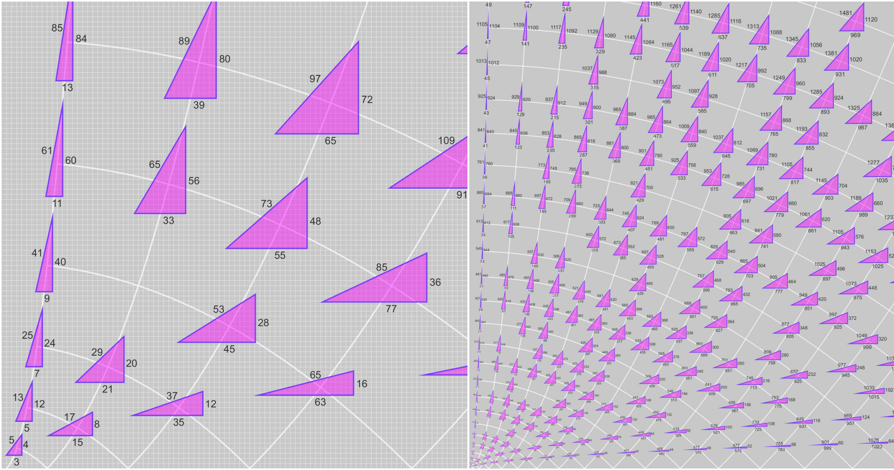


Figure : Source: Wikipedia

What numbers can be factors of a, b, and c?

Theorem

Exactly one of a and b is divisible by three.

Proof.

If both were divisible by three, then c would be also.
If neither are divisible by three, then they equal one or two mod 3.
$(3k+1)^2 = 9k^2 + 6k + 1$
$(3k+2)^2 = 9k^2 + 12k + 4$
Thus a^2 and b^2 both equal 1 mod 3, so $c^2 \equiv 2$ mod 3, which is impossible. $\square$

- Exactly one of a and b is divisible by 4.
- Exactly one of a, b, and c is divisible by 5.

What numbers can be contained in Pythagorean triples?

Theorem

An integer $r > 1$ is a leg of some primitive Pythagorean triple $\iff$ $r \neq 2 \pmod 4$.

Proof.

($\Leftarrow$) Let r be odd. Then $\left(r, \frac{r^2-1}{2}, \frac{r^2+1}{2}\right)$ is a Pythagorean triple. It is primitive since if p divides r, p does not divide $r+1$ or $r-1$.
Let $r = 4k$. Then $(4k^2-1, 4k, 4k^2+1)$ is a Pythagorean triple which is primitive since if p divides $2k$, it does not divide $2k+1$ or $2k-1$.
($\Rightarrow$) Let $r \equiv 2 \pmod 4$. Then n is even, but not divisible by 4. Then r is not a, so if it is b, then $r = 2mn$. But one of m and n are even, so r is not b either. $\square$

Thus 6, 10, 14, ... are not legs of any primitive Pythagorean triple.

Fermat's Theorem

To determine whether an integer can be a hypotenuse of a Pythagorean triple, we need another theorem first.

Theorem

[Fermat's Theorem on the Sums of Squares] The prime p is the sum of two integer squares, $p = a^2 + b^2 \iff p = 2$ or $p \equiv 1 \pmod 4$.

- For example, $2 = 1 + 1$, $5 = 4 + 1$, $13 = 9 + 4$, $17 = 16 + 1$, $29 = 25 + 4$, $37 = 36 + 1$, and $41 = 25 + 16$.
- However, 3, 7, 11, 19, 23, 31, 43, ... are not sums of two squares.

We need a corollary of this theorem.

Corollary

Let $n = 2^k p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s}$ be a positive integer where the factors are all primes and $p_i \equiv 1 \pmod 4$ and $q_i \equiv 3 \pmod 4$. Then $n = A^2 + B^2 \iff$ each b_i is even. In this case, n can be represented as a sum of squares in $4(a_1 + 1) \cdots (a_r + 1)$ ways.

- For example, $65 = 5 \cdot 13 = 64 + 1 = 49 + 16$. Interchanging and allowing negatives produces the 16 possibilities.
- These results can be proved using Gaussian integers, which we will not examine in this talk.

Theorem

An integer $r > 1$ is the hypotenuse of some primitive Pythagorean triple $\iff$ any prime factor p of r satisfies $p \equiv 1 \pmod 4$.

Proof.

($\Leftarrow$) By Corollary 8, r can be expressed as a sum of squares, $r = m^2 + n^2$. The facts that $m > n > 0$, m and n are relatively prime, and m and n have opposite parity can be checked using the proof of Corollary 8.

($\Rightarrow$) Assume $p \neq 1 \pmod 4$. If $p = 2$, then p does not divide n, since n is odd. If $p = 3 \pmod 4$, then by Corollary 8, p^2 divides n. But $\frac{n}{p^2}$ can be expressed as a sum of squares the same number of ways, so if $\frac{n}{p^2} = m^2 + n^2$, then $n = (pm)^2 + (pn)^2$. Thus the triple is not primitive, so p does not divide n. $\square$

Thus $65 = 5 \cdot 13$ is the hypotenuse of $(63, 16, 65)$, but $11 = 4 \cdot 2 + 3$ and $49 = 7^2$ are not the hypotenuses of any primitive triple.

Enumerating Pythagorean Triples

Theorem

Let r be an integer, $r \neq 2 \pmod 4$, with k distinct prime factors. Then r is a leg of 2^{k-1} different primitive Pythagorean triples.

Proof.

Let r be even, so 4 divides n. Then $r = 2mn$, and one of m and n is even, so 2 divides mn. Thus mn has the same number of distinct prime factors as r. Now $r = 2^k p_1^{a_1} \cdots p_r^{a_r}$. We want all possible factorizations of $\frac{r}{2}$ into m and n, which are relatively prime. Thus if p_i divides m, so does $p_i^{a_i}$. Since there are k distinct factors, there are 2^k possibilities. But every possible factorization is counted twice, so there are 2^{k-1} ways that r occurs in Pythagorean triples. Let r be odd. Then $r = m^2 - n^2 = (m+n)(m-n)$. Thus $m+n$ and $m-n$ are odd. If they had a common odd factor, it would divide their sum $2m$ and difference $2n$, a contradiction. Thus we want all possible factorizations of r into two relatively prime factors. As with the even case, there are 2^{k-1} ways to do this. □

For example, $60 = 2^2 3 \cdot 5$ is a leg in four triples: $(11, 60, 61)$, $(91, 60, 109)$, $(221, 60, 229)$, and $(899, 60, 901)$.

Theorem

Let r be an integer with k distinct prime factors such that any prime factor p of r satisfies $p \equiv 1 \pmod 4$. Then r is the hypotenuse of 2^{k-1} different primitive Pythagorean triples.

Thus $65 = 5 \cdot 13$ is the hypotenuse of $(63, 16, 65)$ and $(33, 56, 65)$.

Corollary

An integer occurs r times as a leg or hypotenuse of a primitive Pythagorean triple $\iff r = 2^{k-1}$ for some integer k.
No number occurs infinitely many times as a leg or hypotenuse of a primitive Pythagorean triple.
For all N, there exists r such that r occurs more than N times as a leg or hypotenuse of a primitive Pythagorean triple.

Furthermore,

Corollary

The smallest even number to occur as a leg of a primitive Pythagorean triple 2^{k-1} times is 2 times the product of the first k distinct primes.
The smallest odd number to occur as a leg of a primitive Pythagorean triple 2^{k-1} times is the product of the first k distinct odd primes.
The smallest number to occur as the hypotenuse of a primitive Pythagorean triple 2^{k-1} times is the product of the first k distinct primes that are congruent to 1 (mod 4).

What about non-primitive triples?

Theorem

The number of ways that an integer $r = 2^j p_1^{a_1} \cdots p_k^{a_k}$ occurs as a leg of (not-necessarily primitive) Pythagorean triples is

$$\begin{cases} \frac{1}{2}\left(\prod(2a_i+1)-1\right) & r odd \\ \left(j-\frac{1}{2}\right)\prod(2a_i+1)-\frac{1}{2} & r even \end{cases}.$$

- For example, $15 = 3 \cdot 5$ is a leg of four triples: $5(3,4,5)$, $3(5,12,13)$, $(15,8,17)$, and $(15,112,113)$.
- For example, $12 = 2^2 3$ is a leg of four triples: $3(3,4,5)$, $4(3,4,5)$, $(5,12,13)$, and $(35,12,37)$.

Enumerating Pythagorean Triples

Theorem

The number of ways that an integer $r = 2^j p_1^{a_1} \cdots p_k^{a_k} q_1^{b_1} \cdots q_l^{b_l}$ where the factors are all primes and $p_i \equiv 1 \pmod 4$ and $q_i \equiv 3 \pmod 4$ occurs as the hypotenuse of (not-necessarily primitive) Pythagorean triples is $\frac{1}{2}\left(\prod(2a_i+1)-1\right)$.

- For example, $65 = 5 \cdot 13$ is the hypotenuse of four triples: $13(3,4,5)$, $5(5,12,13)$, $(63,16,65)$ and $(33,56,65)$.
- The proofs of the previous two theorems analyze the number of ways to distribute the possible factors.

Consider a Pythagorean triple as a column vector.
Start with (3,4,5) and multiply by the following matrices

$$A = \begin{bmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{bmatrix}, B = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix}, C = \begin{bmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{bmatrix} \begin{bmatrix} 3 \\ 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 5 \\ 12 \\ 13 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix} \begin{bmatrix} 3 \\ 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 21 \\ 20 \\ 29 \end{bmatrix}$$

$$\begin{bmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{bmatrix} \begin{bmatrix} 3 \\ 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 15 \\ 8 \\ 17 \end{bmatrix}$$

These are all primitive Pythagorean triples!

Consider a Pythagorean triple as a column vector.
Start with $(3,4,5)$ and multiply by the following matrices

$$A = \begin{bmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{bmatrix}, B = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix}, C = \begin{bmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{bmatrix} \begin{bmatrix} 3 \\ 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 5 \\ 12 \\ 13 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix} \begin{bmatrix} 3 \\ 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 21 \\ 20 \\ 29 \end{bmatrix}$$

$$\begin{bmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{bmatrix} \begin{bmatrix} 3 \\ 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 15 \\ 8 \\ 17 \end{bmatrix}$$

These are all primitive Pythagorean triples!

Triples and Matrices

It is possible to generate all primitive Pythagorean triples this way.

(3,4,5)	(5,12,13)	(7,24,25)	(9,40,41)
			(105,88,137)
			(91,60,109)
		(55,48,73)	(105,208,233)
			(297,304,425)
			(187,84,205)
		(45,28,53)	(95,168,193)
			(207,224,305)
			(117,44,125)
	(21,20,29)	(39,80,89)	(57,176,185)
			(377,336,505)
			(299,180,349)
		(119,120,169)	(217,456,505)
			(697,696,985)
			(495,220,509)
		(77,36,85)	(175,288,337)
			(319,360,481)
			(165,52,173)
	(15,8,17)	(33,56,65)	(51,140,149)
			(275,252,373)
			(209,120,241)
		(65,72,97)	(115,252,277)
			(403,396,565)
			(273,136,305)
		(35,12,37)	(85,132,157)
			(133,156,205)
			(63,16,65)

Note that special cases are produced by multiplying by only one of A, B, or C.

- $(3,4,5)\,A^k$: $\left(r, \frac{r^2-1}{2}, \frac{r^2+1}{2}\right)$, $r = 2k+1$
- $(3,4,5)\,B^k$: $b - a = (-1)^k$
- $(3,4,5)\,C^k$: $(4k^2-1, 4k, 4k^2+1)$

To check that a Pythagorean triple is produced by A, we see

$$\begin{bmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} a-2b+2c \\ 2a-b+2c \\ 2a-2b+3c \end{bmatrix}$$

$$\begin{aligned}
&(a-2b+2c)^2 + (2a-b+2c)^2 \\
&= (a^2+4b^2+4c^2-4ab+4ac-8bc) + \\
&\quad (4a^2+b^2+4c^2-4ab+8ac-4bc) \\
&= 5a^2+5b^2+8c^2-8ab+12ac-12bc \text{ (since } a^2+b^2=c^2) \\
&= 4a^2+4b^2+9c^2-8ab+12ac-12bc = (2a-2b+3c)^2
\end{aligned}$$

Matrices B and C can be similarly checked.

Note that special cases are produced by multiplying by only one of A, B, or C.

- $(3,4,5)\,A^k$: $\left(r, \frac{r^2-1}{2}, \frac{r^2+1}{2}\right)$, $r = 2k+1$
- $(3,4,5)\,B^k$: $b - a = (-1)^k$
- $(3,4,5)\,C^k$: $(4k^2-1, 4k, 4k^2+1)$

To check that a Pythagorean triple is produced by A, we see

$$\begin{bmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} a-2b+2c \\ 2a-b+2c \\ 2a-2b+3c \end{bmatrix}$$

$$\begin{aligned}
&(a-2b+2c)^2 + (2a-b+2c)^2 \\
&= \left(a^2+4b^2+4c^2-4ab+4ac-8bc\right) + \\
&\quad \left(4a^2+b^2+4c^2-4ab+8ac-4bc\right) \\
&= 5a^2+5b^2+8c^2-8ab+12ac-12bc \text{ (since } a^2+b^2=c^2) \\
&= 4a^2+4b^2+9c^2-8ab+12ac-12bc = (2a-2b+3c)^2
\end{aligned}$$

Matrices B and C can be similarly checked.

Triples and Matrices

- Why is the triple primitive?
- The three matrices are unimodular–that is, they have integer entries and determinant ± 1.
- Thus their inverses are also unimodular.
- Now if $(d, e, f) = A(a, b, c)$, then $(a, b, c) = A^{-1}(d, e, f)$.
- Thus if d, e, and f have a common factor, then a, b, and c must also.
- To show that each triple is obtained only once, we show that there is only one path back to (3,4,5).
- For each triple, only one of the three inverse matrices A^{-1}, B^{-1}, and C^{-1} yields all positive entries and a smaller hypotenuse.
- By induction, there is only one path from the triple to (3,4,5), and hence the reverse is also true.

Triples and Matrices

- Why is the triple primitive?
- The three matrices are unimodular–that is, they have integer entries and determinant ± 1.
- Thus their inverses are also unimodular.
- Now if $(d,e,f) = A(a,b,c)$, then $(a,b,c) = A^{-1}(d,e,f)$.
- Thus if d, e, and f have a common factor, then a, b, and c must also.

- To show that each triple is obtained only once, we show that there is only one path back to $(3,4,5)$.
- For each triple, only one of the three inverse matrices A^{-1}, B^{-1}, and C^{-1} yields all positive entries and a smaller hypotenuse.
- By induction, there is only one path from the triple to $(3,4,5)$, and hence the reverse is also true.

- There are many generalizations of Pythagorean triples.
- Pythagorean Quadruples: $a^2 + b^2 + c^2 = d^2$
- Examples:
- $(1, 2, 2, 3)$, since $1^2 + 2^2 + 2^2 = 3^2$
- $(2, 3, 6, 7)$, since $2^2 + 3^2 + 6^2 = 7^2$
- These are all given by the formula $\left(m^2 + n^2 - p^2 - q^2\right)^2 + (2mq + 2np)^2 + (2nq - 2mp)^2 = \left(m^2 + n^2 + p^2 + q^2\right)^2$.
- This can be generalized to Pythagorean n-tuples.

Heronian Triples

- Heron's formula for the area of a triangle says that $A = \sqrt{s(s-a)(s-b)(s-c)}$.
- A Heronian triangle is one for which a, b, and c and A are integers.
- Any Pythagorean triple is a Heronian triple, since $A = \frac{1}{2}ab$, and one of a and b must be even.
- However, there are other examples:
- (4, 13, 15) with area 24
- (3, 25, 26) with area 36
- (7, 15, 20) with area 42
- (6, 25, 29) with area 60
- Heron's formula requires that $(a^2+b^2+c^2)^2-2(a^4+b^4+c^4)$ be a nonzero perfect square divisible by 16.

- In 1637, Pierre de Fermat asserted Fermat's Last Theorem:

Theorem

[Fermat's Last Theorem] There are no positive integer solutions (x, y, z) *to*

$$x^n + y^n = z^n$$

for any integer $n > 2$.

- Fermat claimed to have proven this theorem, but that the margin of the book he was reading was too small to contain the proof.
- For 358 years no proof was found. Many mathematicians tried to find a proof, whether Fermat's or something else.
- For a long time this was perhaps the most famous unsolved problem in mathematics.

- Many partial results were obtained, and the result was proved for specific values of n. However, a full proof remained elusive.
- This quest motivated much of the development of the subject of number theory.
- Finally in 1995, after seven years of work, British mathematician Andrew Wiles announced a proof.
- His paper was 125 pages long, and employed very difficult mathematics.
- This talk is definitely too small to contain Wiles' proof!

- Many partial results were obtained, and the result was proved for specific values of n. However, a full proof remained elusive.
- This quest motivated much of the development of the subject of number theory.
- Finally in 1995, after seven years of work, British mathematician Andrew Wiles announced a proof.
- His paper was 125 pages long, and employed very difficult mathematics.
- This talk is definitely too small to contain Wiles' proof!

Sources:

- An Introduction to Number Theory by Harold M. Stark
- Abstract Algebra, 3rd Ed. by Dummit and Foote
- Wikipedia