Pythagoras hits the prime time!

Dr Edward Crane

University of Bristol

February 11, 2015

Distances between grid points

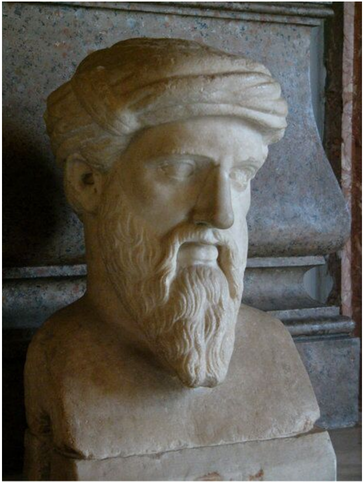
Imagine you have a very large piece of squared paper, say with centimetre squares.

If you measure the distance between two grid points, what are the possible answers?

Pythagoras

Here's what Pythagoras may have looked like. (At least the headgear and beard are probably right). This bust is in the Capitoline museum in Rome. He lived from about 570 BC to about 495 BC.

Pythagoras founded a religious sect who loved mathematics and philosophy, and they probably knew how to calculate the hypotenuse of a right-angled triangle. But there's no evidence that Pythagoras himself ever proved a theorem!



The Pythagorean theorem

The Pythagorean's weren't even the first people to know how to calculate the length of the long side of a right-angled triangle. It was known earlier in India and in Babylon.

Getting back to those distances between grid points, the distances we can measure are exactly the numbers d that can be written as

$$d = \sqrt{x^2 + y^2},$$

where x and y are whole numbers, also known as *integers*.

The first few distances

$$\sqrt{0}, \sqrt{1}, \sqrt{2}, \sqrt{4}, \sqrt{5}, \sqrt{8}, \sqrt{9}, \sqrt{10}, \sqrt{13}, \sqrt{16}, \sqrt{17}, \sqrt{18}, \sqrt{20}, \ldots$$

Is there a pattern?

A more precise question

If you give me a distance d, how can I decide whether it is the distance between two grid points?

The first thing to check is whether d^2 is an integer. If not, then d is not the distance between two grid points.

So the interesting question is,

"Which positive integers are equal to the sum of two squares?"

Let's start by looking at some small examples:

$$
\begin{aligned}
0 &= 0^2 + 0^2 \\
1 &= 1^2 + 0^2 \\
2 &= 1^2 + 1^2 \\
3 & \\
4 &= 2^2 + 0^2 \\
5 &= 2^2 + 1^2 \\
6 & \\
7 & \\
8 &= 2^2 + 2^2 \\
9 &= 3^2 + 0^2 \\
10 &= 3^2 + 1^2
\end{aligned}
$$

A few more cases (blue = sum of two squares)

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59

Can you see any patterns?

Now in columns corresponding to values (mod 12)

0	1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31	32	33	34	35
36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69	70	71
72	73	74	75	76	77	78	79	80	81	82	83
84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107

Can you see any patterns here that you didn't notice before?

A bit further...

0	1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31	32	33	34	35
36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69	70	71
72	73	74	75	76	77	78	79	80	81	82	83
84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107
108	109	110	111	112	113	114	115	116	117	118	119
120	121	122	123	124	125	126	127	128	129	130	131
132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155

From patterns to proofs

We spotted lots of different patterns. How can we tell which patterns continue to hold no matter how far we look?

We'll need to prove that our guesses are correct.

For that we need to use some mathematics called *number theory*.

Our most important tool will be *modular arithmetic*, also called *clock arithmetic*.

Modular arithmetic

We say that x is *congruent to* $y \pmod{n}$ when $x - y$ is a multiple of n. That is, x and y leave the same remainder when you divide them both by n.

We write this as

$$x \equiv y \pmod{n}$$

It means there's an integer (whole number) k such that

$$x - y \; = \; k\, n$$

So we could also write the same thing as $n \,|\, (x - y)$.

We read this out as "n divides $x - y$".

For example, $3 \equiv 15 \pmod{12}$.

Modular arithmetic

In the equation $3 \equiv 15 \pmod{12}$, the number 12 is called the *modulus*.

We can do addition, multiplication and subtraction $(\mathrm{mod}\ n)$.

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then

$$\begin{aligned} a+c &\equiv b+d \pmod{n}, \\ a-c &\equiv b-d \pmod{n}, \quad \text{and} \\ ac &\equiv bd \pmod{n}. \end{aligned}$$

To prove the last one, $ac - bd = (a-b)c + b(c-d)$.

The red factors are both multiples of n.

Squares (mod 4)

What are the possible values of $x^2 \pmod 4$ when x is an integer?

If x is even then x^2 is a multiple of 4, so $x^2 \equiv 0 \pmod 4$.

If x is odd then $x = 2y + 1$ for some integer y. Then

$$(2y+1)^2 = 4y^2 + 4y + 1 \equiv 1 \pmod 4 .$$

So squares are always congruent to 0 or 1 (mod 4).

Sums of two squares (mod 4)

The possible values of $x^2 + y^2 \pmod 4$ are

$$\begin{aligned} 0+0 &\equiv 0 \pmod 4 \\ 0+1 &\equiv 1 \pmod 4 \\ 1+0 &\equiv 1 \pmod 4 \\ 1+1 &\equiv 2 \pmod 4 \end{aligned}$$

So we can never get $x^2 + y^2 \equiv 3 \pmod 4$.

Another view - columns correspond to values (mod 9)

0	1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26
27	28	29	30	31	32	33	34	35
36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53
54	55	56	57	58	59	60	61	62
63	64	65	66	67	68	69	70	71
72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98

Can you see any interesting columns this time?

What if $3 \mid n$ and $n = x^2 + y^2$?

What are the possible squares (mod 3)?

What if $3 \mid n$ and $n = x^2 + y^2$?

What are the possible squares (mod 3)?

Only 0 and 1.

How can two of these add up to 0 (mod 3)?

What if $3 \mid n$ and $n = x^2 + y^2$?

Then we must have $x \equiv 0 \pmod 3$ and $y \equiv 0 \pmod 3$.

So $x = 3a$ and $y = 3b$ for some integers a and b, and

$$x^2 + y^2 = (3a)^2 + (3b)^2 = 9(a^2 + b^2)\,.$$

Therefore $9 \mid n$.

So we can't have $x^2 + y^2 \equiv 3 \pmod 9$,

and we can't have $x^2 + y^2 \equiv 6 \pmod 9$.

A different view - the multiplication table

×	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11
2	2	4	6	8	10	12	14	16	18	20	22
3	3	6	9	12	15	18	21	24	27	30	33
4	4	8	12	16	20	24	28	32	36	40	44
5	5	10	15	20	25	30	35	40	45	50	55
6	6	12	18	24	30	36	42	48	54	60	66
7	7	14	21	28	35	42	49	56	63	70	77
8	8	16	24	32	40	48	56	64	72	80	88
9	9	18	27	36	45	54	63	72	81	90	99
10	10	20	30	40	50	60	70	80	90	100	110
11	11	22	33	44	55	66	77	88	99	110	121

A guess

×	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11
2	2	4	6	8	10	12	14	16	18	20	22
3	3	6	9	12	15	18	21	24	27	30	33
4	4	8	12	16	20	24	28	32	36	40	44
5	5	10	15	20	25	30	35	40	45	50	55
6	6	12	18	24	30	36	42	48	54	60	66
7	7	14	21	28	35	42	49	56	63	70	77
8	8	16	24	32	40	48	56	64	72	80	88
9	9	18	27	36	45	54	63	72	81	90	99
10	10	20	30	40	50	60	70	80	90	100	110
11	11	22	33	44	55	66	77	88	99	110	121

Guess: *blue* × *blue* = *blue* and *blue* × *red* = *red*?

Euler’s identity (*blue* × *blue* = *blue*)

$$(x^2 + y^2)(a^2 + b^2) = (xa - yb)^2 + (xb + ya)^2\,.$$

Euler was a Swiss mathematician and physicist who lived from 1707 to 1783. He worked at the imperial court in St Petersburg, and moved in 1741 to Berlin to work for the Prussian emperor Frederick the Great. He was one of the most prolific mathematicians ever.

Squares (mod 7)

The possible squares (mod 7) are 0, 1, 2 and 4.

Squares (mod 7)

The possible squares (mod 7) are 0, 1, 2 and 4.

How can two of these add up to 0 (mod 7)?

What if $7 \mid n$ and $n = x^2 + y^2$?

Then we must have $x \equiv 0 \pmod 7$ and $y \equiv 0 \pmod 7$.

So $x = 7a$ and $y = 7b$ for some integers a and b, and

$$x^2 + y^2 = (7a)^2 + (7b)^2 = 49(a^2 + b^2) \,.$$

Therefore $49 \mid n$. We have proved that

$$7 \mid (x^2 + y^2) \implies 49 \mid (x^2 + y^2) \,.$$

Squares (mod 11)

$$\{0, 1, 3, 4, 5, 9\}$$

Squares (mod 11)

$$\{0, 1, 3, 4, 5, 9\}$$

How can two of these add up to 0 (mod 11)?

Squares (mod 11)

$$\{0, 1, 3, 4, 5, 9\}$$

How can two of these add up to 0 (mod 11)?

$$11 \mid x^2 + y^2 \implies 11^2 \mid x^2 + y^2 \,.$$

Squares (mod 19)

$$\{0, 1, 4, 5, 6, 7, 9, 11, 16, 17\}$$

Squares (mod 19)

$$\{0, 1, 4, 5, 6, 7, 9, 11, 16, 17\}$$

How can two of these add up to 0 (mod 19)?

Squares (mod 19)

$$\{0, 1, 4, 5, 6, 7, 9, 11, 16, 17\}$$

How can two of these add up to 0 (mod 19)?

$$19 \mid x^2 + y^2 \implies 19^2 \mid x^2 + y^2 \,.$$

What about division?

In modular arithmetic we can *sometimes* do division, but not always.

For example $3 \equiv 15 \pmod{12}$ but we can't divide both sides by 3 because $1 \not\equiv 5 \pmod{12}$.

The problem here was that 3 was also a factor of the modulus.

Modular division

Suppose we want to divide by c when we are working modulo n.

We *can* do it if c is not zero and c is *coprime* to the modulus n. That means that they don't have any factors in common other than 1.

A different way to say this is that the *highest common factor* or *greatest common divisor* of c and n is 1:

$$\gcd(c, n) = \mathrm{hcf}(c, n) = 1\,.$$

Euclid’s algorithm

Euclid was a Greek who lived in Alexandria (now in Egypt) around 300 B.C.

He is famous for *The Elements*, a book in which theorems about geometry were deduced carefully from a small set of initial assumptions called *axioms*.

Given integers c and n, *Euclid’s algorithm* enables us to find integers r and s such that

$$rc + sn = \gcd(c, n)\,.$$

Modular division again

If $\gcd(c, n) = 1$ then Euclid's algorithm gives us $rc + sn = 1$, so

$$rc \equiv 1 \pmod{n}$$

Now if we want to divide by $c \pmod{n}$, instead we multiply by r.

If $cx \equiv y \pmod{n}$ then

$$x \equiv (rc)x = r(cx) \equiv ry \pmod{n}.$$

In particular we can do this if n is prime and $c \not\equiv 0 \pmod{n}$.

Fermat's little theorem

Pierre de Fermat (1601 - 1655) was a French lawyer who is most famous for his mathematics - in particular a certain comment in a margin!
Here's a fact that he actually did prove:

If p is prime and $a \not\equiv 0 \pmod{p}$ then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Fermat's little theorem

To prove Fermat's little theorem, consider

$$(p-1)!\, a^{p-1} \;=\; (a)(2a)(3a)\ldots((p-1)a)\,.$$

When you reduce them (mod p), the factors on the right-hand side are exactly the numbers $1, \ldots, p-1$, in some order. To see this, it is enough to check that they are all non-zero and all distinct. So the right-hand side is just $(p-1)!$ again. Therefore

$$(p-1)! a^{p-1} \equiv (p-1)! \pmod{p}\,.$$

Because p is prime, p does not divide $(p-1)!$ so this implies

$$a^{p-1} \equiv 1 \pmod{p}\,.$$

Generalizing from $3, 7, 11, 19 \ldots$

Suppose $x^2 + y^2 \equiv 0 \pmod p$, where p is an *odd prime*.

Also suppose $y \not\equiv 0 \pmod p$. Then

$$x^2 \equiv -y^2 \pmod p$$

and we can find r such that

$$ry \equiv 1 \pmod p\,.$$

So

$$(rx)^2 = r^2x^2 \equiv -r^2y^2 = -(ry)^2 \equiv -1 \pmod p\,.$$

Generalizing from $3, 7, 11, 19 \ldots$

Suppose $x^2 + y^2 \equiv 0 \pmod{p}$, where p is an *odd prime*.

Also suppose $y \not\equiv 0 \pmod{p}$. Then

$$x^2 \equiv -y^2 \pmod{p}$$

and we can find r such that

$$ry \equiv 1 \pmod{p}.$$

So

$$(rx)^2 = r^2x^2 \equiv -r^2y^2 = -(ry)^2 \equiv -1 \pmod{p}.$$

Now raise both sides to the power $(p-1)/2$ and use Fermat's little theorem:

$$1 \equiv (rx)^{p-1} \equiv (-1)^{(p-1)/2} \pmod{p}.$$

This implies that $(p-1)/2$ is even. That is, $p \equiv 1 \pmod{4}$.

What we just proved, stated differently

If p is a prime such that $p \equiv 3 \pmod 4$ then

$$p \mid x^2 + y^2 \implies p \mid y \text{ and } p \mid x\,.$$

In this case, $x^2 + y^2 = p^2(a^2 + b^2)$ for some integers a and b.

It follows that p can only divide a sum of two squares to an *even power*.

What about primes congruent to 1 (mod 4)?

Here are the first few of them:

$$\begin{aligned}
5 &= 2^2 + 1^2 \\
13 &= 3^2 + 2^2 \\
17 &= 4^2 + 1^2 \\
29 &= 5^2 + 2^2 \\
37 &= 6^2 + 1^2 \\
41 &= 5^2 + 4^2 \\
53 &= 7^2 + 2^2 \\
61 &= 6^2 + 5^2 \\
73 &= 8^2 + 3^2 \\
89 &= 8^2 + 5^2
\end{aligned}$$

Wilson's theorem

Here's a theorem that was first stated by Ibn al-Haytham around 1000 AD, and was rediscovered in Europe by Edward Waring and John Wilson in 1770 first proved by Lagrange in 1771. So it is a bit unfair that we call it Wilson's theorem!

If p is prime then $(p-1)! \equiv -1 \pmod{p}$.

Proof: We can arrange the numbers from 2 to $p-2$ into pairs (a, b) where $ab \equiv 1 \pmod{p}$. Multiplying them all together gives us $1 \pmod{p}$. That leaves just 1 and -1 in the factorial.

An application of Wilson's theorem

If $p = 4k + 1$ is a prime then

$$\begin{aligned} -1 \equiv (4k)! &\equiv (1.2.3\ldots 2k)((-2k)(-(2k-1))\ldots(-1)) \\ &\equiv ((2k)!)^2(-1)^{2k} \equiv ((2k)!)^2 \pmod{p} \end{aligned}$$

So we have found an integer m such that $m^2 \equiv -1 \pmod{p}$.

From $m^2 \equiv -1 \pmod{p}$ to $p = x^2 + y^2$

Sort the numbers $m, 2m, 3m, \ldots, \lceil \sqrt{p} \rceil m$, reduced $\pmod{p}$. There are more than $\sqrt{p}$ of them all between 1 and $p-1$, so there must be two of them, say am and bm, that are quite close together around the $\pmod{p}$ clock:

$$(a-b)m \equiv am - bm \equiv c \pmod{p}$$

where

$$|a-b| \leq \lceil \sqrt{p} \rceil - 1 < \sqrt{p}$$

and

$$1 \leq c \leq \frac{p}{\lceil \sqrt{p} \rceil} < \sqrt{p}$$

From $m^2 \equiv -1 \pmod{p}$ to $p = x^2 + y^2$

Squaring we get

$$c^2 \equiv (a-b)^2 m^2 \equiv -(a-b)^2 \pmod{p}$$

so

$$c^2 + (a-b)^2 \equiv 0 \pmod{p}$$

but

$$0 < c^2 + (a-b)^2 < \sqrt{p}^2 + \sqrt{p}^2 = 2p$$

and therefore

$$c^2 + (a-b)^2 = p\,.$$

What we just proved

Every prime congruent to 1 (mod 4) is a sum of two squares.

So is 2.

Every positive integer can be expressed in only one way as a product of powers of primes.

A prime congruent to 3 (mod 4) can only divide $x^2 + y^2$ to an even power.

Theorem

A positive integer n is a sum of two squares *if and only if* every prime congruent to 3 (mod 4) that divides n actually appears to an even power in the prime factorization of n.

A large example

Let's take the first prime after 10^{16} that is congruent to $1 \pmod 4$.

It turns out to be $10000000000000061 = 10^{16} + 61$.

Can we write it as a sum of two squares *in practice*?

A large example

Let's take the first prime after 10^{16} that is congruent to $1 \pmod 4$.

It turns out to be $10000000000000061 = 10^{16} + 61$.

Can we write it as a sum of two squares *in practice*?

Yes! Luckily, there are fast algorithms for a computer to find a square root of $-1 \pmod p$ and to find a solution of $x^2 + y^2 = p$ given this square root. The running time for each one is no more than a constant times $(\log p)^3$.

They both use fun bits of number theory, but they would take a whole talk to explain.

$10^{16} + 61$ as a sum of two squares

$$10^{16} + 61 = 50071525^2 + 86561206^2$$

Two even larger examples - to show you I didn't cheat!

$$278663238180609958003^2 + 149488460045237754610^2$$
$$= 100000000000000000000000000000000000000109 = 10^{41} + 109$$

$$3684758713859920604^2 + 4223562448517994405^2$$
$$= 3141592653897932384626433832795028841 = \lfloor 10^{37}\pi \rfloor$$