Pythagoras $\implies$ \$1 million problem

Ken Ono
Emory University

The Pythagorean Theorem

Theorem (Pythagoras)

If (a, b, c) is a right triangle, then

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

The Pythagorean Theorem

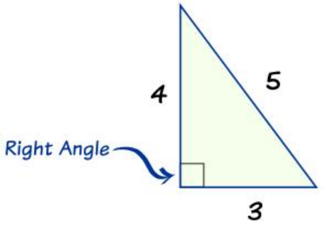
Theorem (Pythagoras)

If (a, b, c) *is a right triangle, then*

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

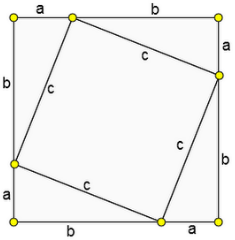
Example

We have:

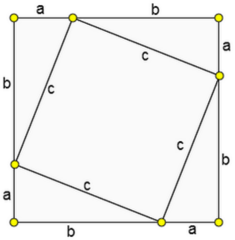


Proof of the Pythagorean Theorem

Proof of the Pythagorean Theorem

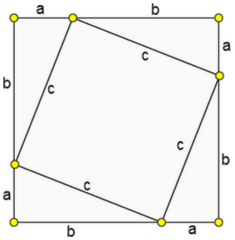


Proof of the Pythagorean Theorem



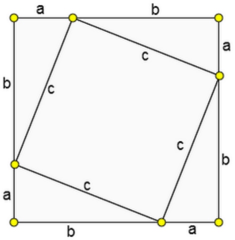
- Four (a, b, c) right triangles and one large $c \times c$ square.

Proof of the Pythagorean Theorem



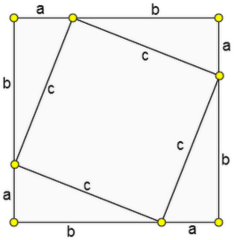
- Four (a, b, c) right triangles and one large $c \times c$ square.
- This has area: $4 \cdot \frac{1}{2}ab + c^2 = 2ab + c^2$.

Proof of the Pythagorean Theorem



- Four (a, b, c) right triangles and one large $c \times c$ square.
- This has area: $4 \cdot \frac{1}{2}ab + c^2 = 2ab + c^2$.
- As one large square, it has area: $(a + b)^2 = a^2 + 2ab + b^2$.

Proof of the Pythagorean Theorem



- Four (a, b, c) right triangles and one large $c \times c$ square.
- This has area: $4 \cdot \frac{1}{2}ab + c^2 = 2ab + c^2$.
- As one large square, it has area: $(a + b)^2 = a^2 + 2ab + b^2$.
- $\Longrightarrow \quad c^2 = a^2 + b^2$.

Definition

Integers (a, b, c) form a **Pythagorean Triple** if $a, b, c > 0$ and

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

Definition

Integers (a, b, c) form a **Pythagorean Triple** if $a, b, c > 0$ and

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

Moreover, it is called **primitive** if $\gcd(a, b, c) = 1$.

Definition

Integers (a, b, c) form a **Pythagorean Triple** if $a, b, c > 0$ and

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

Moreover, it is called **primitive** if $\gcd(a, b, c) = 1$.

Example

The "first few" Pythagorean triples:

$$(3, 4, 5), (5, 12, 13), (2 \cdot 3, 2 \cdot 4, 2 \cdot 5), \ (7, 24, 25), (8, 15, 17), \\ (3 \cdot 3, 3 \cdot 4, 3 \cdot 5) \ldots$$

Definition

Integers (a, b, c) form a **Pythagorean Triple** if $a, b, c > 0$ and

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

Moreover, it is called **primitive** if $\gcd(a, b, c) = 1$.

Example

The "first few" Pythagorean triples:

$$(3,4,5),(5,12,13),(2\cdot 3, 2\cdot 4, 2\cdot 5),\ (7,24,25),(8,15,17),$$
$$(3\cdot 3, 3\cdot 4, 3\cdot 5)\dots$$

The "first few" Primitive Pythagorean Triples:

$$(3,4,5),\ (5,12,13),\ (7,24,25),\ (8,15,17),\ (9,40,41),\dots$$

Natural questions

Natural questions

Question

How many Pythagorean Triples exist?

Natural questions

Question

How many Pythagorean Triples exist?

Answer

Easy...infinitely many because of **scaling.**

Natural questions

Question

How many Pythagorean Triples exist?

Answer

Easy...infinitely many because of **scaling.**

Better Question

How many Primitive Pythagorean Triples exist?

Beautiful Theorem

Beautiful Theorem

Theorem (Euclid)

Every PPT with odd a and even b is of the form

$$(a, b, c) = \left(st, \frac{s^2 - t^2}{2}, \frac{s^2 + t^2}{2}\right)$$

where $s > t \geq 1$ are odd coprime integers.

Beautiful Theorem

Theorem (Euclid)

Every PPT with odd a and even b is of the form

$$(a, b, c) = \left(st, \frac{s^2 - t^2}{2}, \frac{s^2 + t^2}{2} \right)$$

where $s > t \geq 1$ are odd coprime integers.

Example

This theorem is easy to use:

$$(s, t) = (17, 5) \quad \Longrightarrow \quad (a, b, c) = (85, 132, 157).$$

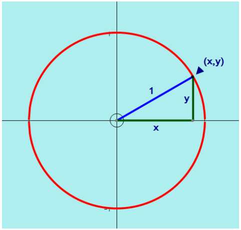
Connection to Unit Circle

Connection to Unit Circle

$$a^2 + b^2 = c^2 \quad \Longrightarrow \quad \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

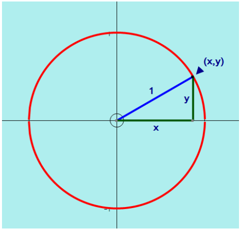
Connection to Unit Circle

$$a^2 + b^2 = c^2 \quad \Longrightarrow \quad \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$



Connection to Unit Circle

$$a^2 + b^2 = c^2 \quad \Longrightarrow \quad \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$



Question

How do we find all the **rational points** *(i.e. x, y rational numbers) on the unit circle?*

Sample points...

Sample points...

Obvious rational points on the unit circle:

$$(\pm 1, 0) \quad \text{and} \quad (0, \pm 1).$$

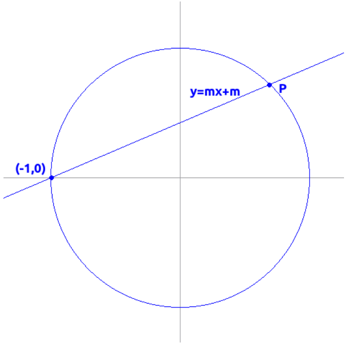
Sample points...

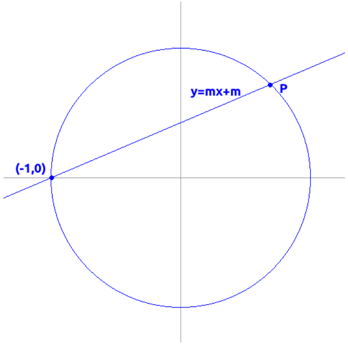
Obvious rational points on the unit circle:

$$(\pm 1, 0) \quad \text{and} \quad (0, \pm 1).$$

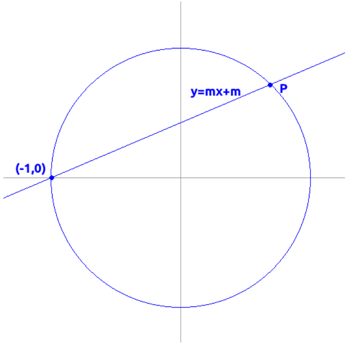
Some much less obvious points:

$$\left(-\frac{4}{5}, \frac{3}{5}\right), \left(\frac{45}{53}, \frac{28}{53}\right), \quad \ldots, \quad \left(\frac{231660}{245821}, \frac{82229}{245821}\right), \ldots$$

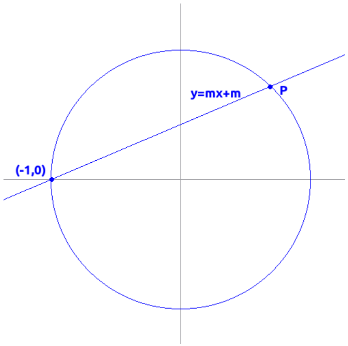

y=mx+m
P
(-1,0)



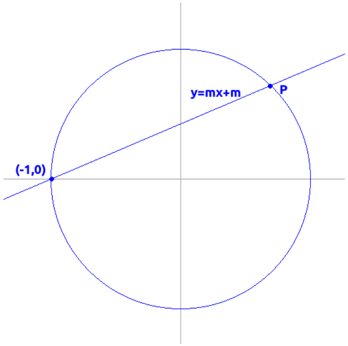
- Rational pts $P \neq (-1, 0)$ have lines with **rational** slopes m.



- Rational pts $P \neq (-1, 0)$ have lines with **rational** slopes m.
- By substituting $y = mx + m$ into $x^2 + y^2 = 1$
  $\Longrightarrow \quad x^2 + (mx + m)^2 = 1.$



- Rational pts $P \neq (-1, 0)$ have lines with **rational** slopes m.
- By substituting $y = mx + m$ into $x^2 + y^2 = 1$
  $\Longrightarrow \quad x^2 + (mx + m)^2 = 1.$
- One root is $x = -1$



- Rational pts $P \neq (-1, 0)$ have lines with **rational** slopes m.
- By substituting $y = mx + m$ into $x^2 + y^2 = 1$
  $\Longrightarrow \quad x^2 + (mx + m)^2 = 1.$
- One root is $x = -1$ and the other gives $P = \left(\frac{1-m^2}{m^2+1}, \frac{2m}{m^2+1}\right)$.

Rational Points

Theorem (Chord Method)

The rational points on the unit circle are:

$$(-1,0) \cup \left\{ \left(\frac{1-m^2}{m^2+1}, \frac{2m}{m^2+1} \right) \; : \; m \text{ rational} \right\}.$$

Rational Points

Theorem (Chord Method)

The rational points on the unit circle are:

$$(-1,0) \cup \left\{ \left(\frac{1-m^2}{m^2+1}, \frac{2m}{m^2+1} \right) \ : \ m \text{ rational} \right\}.$$

Remark

By **drawing** *and* **intersecting** *lines, we determined* **all** *the rational points from a* **single** *point* $(-1,0)$.

Natural Questions

Natural Questions

- Can one solve other *Diophantine* equations from a **finite seed set of points** by intersecting lines?

Natural Questions

- Can one solve other *Diophantine* equations from a **finite seed set of points** by intersecting lines?
- How many points are needed for starters?

Natural Questions

- Can one solve other *Diophantine* equations from a **finite seed set of points** by intersecting lines?
- How many points are needed for starters?
- What if one **cannot find** any points to start with?

An ancient problem

Definition

An integer is **congruent** if it is the area of a right triangle with rational sidelengths.

An ancient problem

Definition

An integer is **congruent** if it is the area of a right triangle with rational sidelengths.

Problem (Arab Scholars)

Classify all of the congruent numbers.

Is this an easy problem?

Is this an easy problem?

Example

Here are some facts:

Is this an easy problem?

Example

Here are some facts:

- 6 is congruent thanks to $(3, 4, 5)$.

Is this an easy problem?

Example

Here are some facts:

- 6 is congruent thanks to $(3, 4, 5)$.
- 5 is congruent since

Is this an easy problem?

Example

Here are some facts:

- 6 is congruent thanks to $(3, 4, 5)$.
- 5 is congruent since

$$\left(\frac{3}{2}\right)^2 + \left(\frac{20}{3}\right)^2 = \left(\frac{41}{6}\right)^2 \quad \text{and} \quad \frac{1}{2} \cdot \frac{3}{2} \cdot \frac{20}{3} = 5.$$

Is this an easy problem?

Example

Here are some facts:

- 6 is congruent thanks to $(3, 4, 5)$.
- 5 is congruent since

$$\left(\frac{3}{2}\right)^2 + \left(\frac{20}{3}\right)^2 = \left(\frac{41}{6}\right)^2 \quad \text{and} \quad \frac{1}{2} \cdot \frac{3}{2} \cdot \frac{20}{3} = 5.$$

- 1 **is not** congruent because ???.

Zagier's Example

Zagier's Example

Example

The number 157 is congruent, since it is the area of

$$\left(\frac{411340519227716149383203}{21666555693714761309610}, \frac{680\cdots540}{411\cdots203}, \frac{224\cdots041}{891\cdots830}\right).$$

Zagier's Example

Example

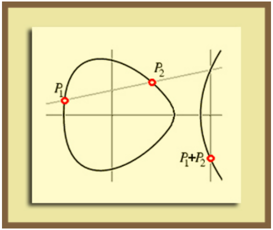
The number 157 is congruent, since it is the area of

$$\left(\frac{411340519227716149383203}{21666555693714761309610}, \frac{680\cdots540}{411\cdots203}, \frac{224\cdots041}{891\cdots830}\right).$$

Remark

The problem of classifying congruent numbers is probably hard.

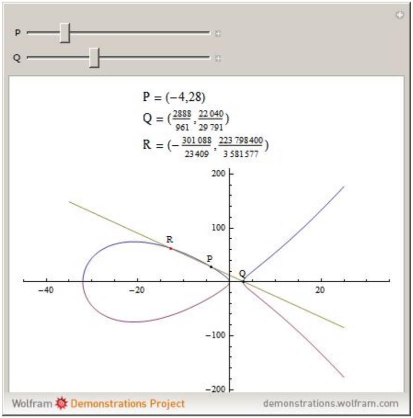
Another Chord Law



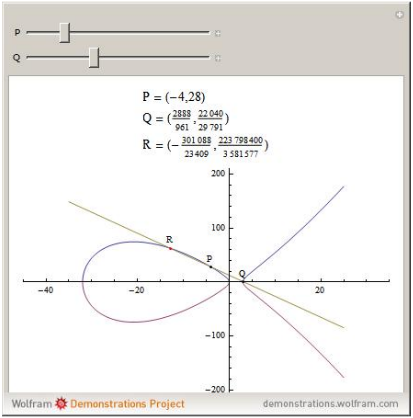
Group Law

$$E \ : \ y^2 = x^3 + Ax + B$$

Example $E : y^2 = x(x-3)(x+32)$



Example $E : y^2 = x(x-3)(x+32)$



We find that $P + Q = \left(-\frac{301088}{23409}, -\frac{223798400}{3581577}\right)$.

Big theorems

Big theorems

Theorem (Classical Fact)

The rational points on an elliptic curve form an abelian group.

Big theorems

Theorem (Classical Fact)

The rational points on an elliptic curve form an abelian group.

Theorem (Mordell)

The rational points of an elliptic curve form a **finitely generated** *abelian group.*

Big theorems

Theorem (Classical Fact)

The rational points on an elliptic curve form an abelian group.

Theorem (Mordell)

The rational points of an elliptic curve form a **finitely generated** *abelian group.*

Question

What kind of groups arise?

Examples of Groups of Rational Points

Examples of Groups of Rational Points

E	Group	# of Finite Pts
$y^2 = x(x-1)(x+1)$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	3
$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$	5
$y^2 = x^3 + 17$	$\mathbb{Z} \times \mathbb{Z}$	∞
$y^2 = x^3 + 17x + 10$	$\mathbb{Z}/1\mathbb{Z}$	0

A Classical Diophantine criterion

A Classical Diophantine criterion

Theorem

An integer D is congruent if and only if the elliptic curve

$$E_D : \quad y^2 = x(x + D)(x - D)$$

has **infinitely many** *points.*

Some data

Some data

Example

The first few congruent numbers:

$$5, 6, 7, 13, 14, 15, 20, 21, 22, 23, \ldots.$$

Some data

Example

The first few congruent numbers:

$$5, 6, 7, 13, 14, 15, 20, 21, 22, 23, \ldots.$$

The first few non-congruent numbers:

$$1, 2, 3, 4, 8, 9, 10, 11, 12, 16, 17, 18, 19, \ldots.$$

Some data

Example

The first few congruent numbers:

$$5, 6, 7, 13, 14, 15, 20, 21, 22, 23, \ldots.$$

The first few non-congruent numbers:

$$1, 2, 3, 4, 8, 9, 10, 11, 12, 16, 17, 18, 19, \ldots.$$

Conjecture

Half of the integers are congruent.

How do we make use of this criterion?

How do we make use of this criterion?

Good question....

How do we make use of this criterion?

Good question....a $1 million question!

\$1 million bounty

Definition (Trace mod p)

For primes p, let

$$a(p) := p - \#\{(x, y) \pmod{p} \ : \ y^2 \equiv x^3 - x \pmod{p}\}.$$

Definition (Trace mod p)

For primes p, let

$$a(p) := p - \#\{(x, y) \pmod p \ : \ y^2 \equiv x^3 - x \pmod p\}.$$

Example

For $p = 7$ we have the 7 points mod 7:

$$\{(0, 0), (1, 0), (4, 2), (4, 5), (5, 1), (5, 6), (6, 0)\}.$$

Definition (Trace mod p)

For primes p, let

$$a(p) := p - \#\{(x, y) \pmod{p} \ : \ y^2 \equiv x^3 - x \pmod{p}\}.$$

Example

For $p = 7$ we have the 7 points mod 7:

$$\{(0,0), (1,0), (4,2), (4,5), (5,1), (5,6), (6,0)\}.$$

$$\Longrightarrow \quad a(7) = 7 - 7 = 0.$$

A very strange phenomenon

Define integers $A(n)$ by

$$\sum_{n=1}^{\infty} A(n)x^n := x\prod_{n=1}^{\infty}(1-x^{4n})^2(1-x^{8n})^2 = x - 2x^5 - 3x^9 + \dots.$$

A very strange phenomenon

Define integers $A(n)$ by

$$\sum_{n=1}^{\infty} A(n)x^n := x \prod_{n=1}^{\infty} (1 - x^{4n})^2 (1 - x^{8n})^2 = x - 2x^5 - 3x^9 + \dots.$$

Then for primes p we have:

A very strange phenomenon

Define integers $A(n)$ by

$$\sum_{n=1}^{\infty} A(n)x^n := x\prod_{n=1}^{\infty}(1-x^{4n})^2(1-x^{8n})^2 = x - 2x^5 - 3x^9 + \dots.$$

Then for primes p we have:

p	3	5	7	11	13	17	19	23	$\cdots$	97
$a(p)$	0	-2	0	0	6	2	0	0	$\cdots$	18
$A(p)$	0	-2	0	0	6	2	0	0	$\cdots$	18

A very strange phenomenon

Define integers $A(n)$ by

$$\sum_{n=1}^{\infty} A(n)x^n := x\prod_{n=1}^{\infty}(1-x^{4n})^2(1-x^{8n})^2 = x - 2x^5 - 3x^9 + \dots.$$

Then for primes p we have:

p	3	5	7	11	13	17	19	23	$\cdots$	97
$a(p)$	0	-2	0	0	6	2	0	0	$\cdots$	18
$A(p)$	0	-2	0	0	6	2	0	0	$\cdots$	18

Theorem (Modularity)

If p is prime, then $A(p) = a(p)$.

The Hasse-Weil Function

The Hasse-Weil Function

For D, define the function

$$L(D,s) := \sum_{n=1}^{\infty} \frac{\left(\frac{D}{n}\right) A(n)}{n^s}.$$

Example

For $D = 1$, we find that

$$L(1,s) = 0.65551\ldots$$

So what?

So what?

D	Congruent (Y/N)	$L(D,1)$
5	Y	0
6	Y	0
7	Y	0
8	N	$0.9270\ldots$
9	N	$0.6555\ldots$
10	N	$1.6583\ldots$
11	N	$0.7905\ldots$
12	N	$1.5138\ldots$
13	Y	0
14	Y	0
15	Y	0

Birch and Swinnerton-Dyer Conjecture

Conjecture

If $E/\mathbb{Q}$ is an elliptic curve and $L(E,s)$ is its L-function, then

$$L(E,1) = 0 \text{ if and only if } \#E(\mathbb{Q}) = +\infty.$$

Birch and Swinnerton-Dyer Conjecture

Conjecture

If $E/\mathbb{Q}$ is an elliptic curve and $L(E,s)$ is its L-function, then

$$L(E,1) = 0 \text{ if and only if } \#E(\mathbb{Q}) = +\infty.$$

Corollary

Assuming BSD, D is congruent iff $L(D,1) = 0$.

Kolyvagin's Theorem

Theorem (Kolyvagin)

If $L(E,1) \neq 0$, then $\#E(\mathbb{Q}) < +\infty$.

Kolyvagin's Theorem

Theorem (Kolyvagin)

If $L(E,1) \neq 0$, *then* $\#E(\mathbb{Q}) < +\infty$.

Remark

If $\mathrm{ord}_{s=1}(L(E,s)) \in \{0,1\}$, *then he proves that this order is the number of "generators".*

A strange "criterion" using **modularity**

A strange "criterion" using **modularity**

Theorem (Tunnell, 1983)

If D is odd and square-free, then $L(D,1)=0$ if and only if

$$\#\{2x^2+y^2+32z^2=D\}=\frac{1}{2}\cdot\#\{2x^2+y^2+8z^2=D\}.$$

A strange "criterion" using **modularity**

Theorem (Tunnell, 1983)

If D is odd and square-free, then $L(D,1)=0$ if and only if

$$\#\{2x^2+y^2+32z^2=D\}=\frac{1}{2}\cdot\#\{2x^2+y^2+8z^2=D\}.$$

In particular, BSD implies that D is congruent iff we have **equality***.*

A strange "criterion" using **modularity**

Theorem (Tunnell, 1983)

If D is odd and square-free, then $L(D,1) = 0$ if and only if

$$\#\{2x^2 + y^2 + 32z^2 = D\} = \frac{1}{2} \cdot \#\{2x^2 + y^2 + 8z^2 = D\}.$$

In particular, BSD implies that D is congruent iff we have **equality**.

Remark

A strange "criterion" using **modularity**

Theorem (Tunnell, 1983)

If D is odd and square-free, then $L(D, 1) = 0$ if and only if

$$\#\{2x^2 + y^2 + 32z^2 = D\} = \frac{1}{2} \cdot \#\{2x^2 + y^2 + 8z^2 = D\}.$$

In particular, BSD implies that D is congruent iff we have **equality**.

Remark

(1) There is a similar criterion for even square-free D.

A strange "criterion" using **modularity**

Theorem (Tunnell, 1983)

If D is odd and square-free, then $L(D,1) = 0$ if and only if

$$\#\{2x^2 + y^2 + 32z^2 = D\} = \frac{1}{2} \cdot \#\{2x^2 + y^2 + 8z^2 = D\}.$$

In particular, BSD implies that D is congruent iff we have **equality***.*

Remark

(1) There is a similar criterion for even square-free D.

(2) By Kolyvagin, **no** *equality $\implies$ D* **is not** *congruent.*

A strange "criterion" using **modularity**

Theorem (Tunnell, 1983)

If D is odd and square-free, then $L(D,1)=0$ if and only if

$$\#\{2x^2+y^2+32z^2=D\}=\frac{1}{2}\cdot\#\{2x^2+y^2+8z^2=D\}.$$

In particular, BSD implies that D is congruent iff we have **equality**.

Remark

(1) There is a similar criterion for even square-free D.

(2) By Kolyvagin, **no** *equality $\Longrightarrow$ D* **is not** *congruent.*

(3) The converse may require solving the \$1 million problem.

Some facts....

Some facts....

- It is easy to classify Pythagorean Triples.

Some facts....

- It is easy to classify Pythagorean Triples.
- ...motivates using "chords" to study rational points.

Some facts....

- It is easy to classify Pythagorean Triples.
- ...motivates using "chords" to study rational points.
- ...morphs into the "chord" law for elliptic curves.

Some facts....

- It is easy to classify Pythagorean Triples.
- ...motivates using "chords" to study rational points.
- ...morphs into the "chord" law for elliptic curves.
- ...hard to classify congruent numbers.

Some facts....

- It is easy to classify Pythagorean Triples.
- ...motivates using "chords" to study rational points.
- ...morphs into the "chord" law for elliptic curves.
- ...hard to classify congruent numbers.
- If we could... maybe we'd win \$1 million!