# *The Mathematics of Designing Good Problems*

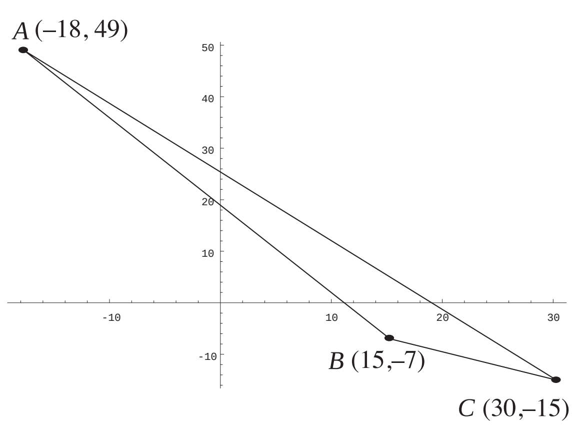
## Prelude

When launching a topic, we look for problems that come out "nice" like these:

**1**. The vertices of a triangle have coordinates

$$(-18, 49), (15, -7), (30, -15)$$

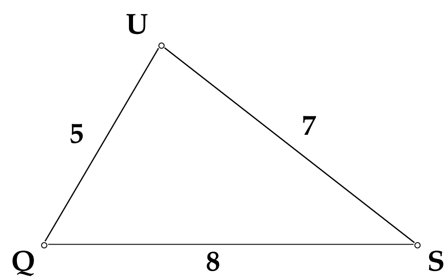
For another one, try the triangle whose vertices are (of course) $(1248, 436), (1500, 500), (-2340, 1548)$.




A strange but nice triangle

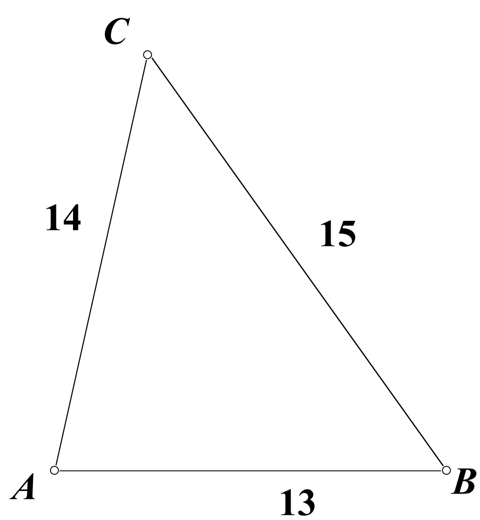
How long are the sides?

**2**. Find m$\angle Q$




Want another? Find the angle opposite the side of length 21 in a triangle whose sides have length $9, 24, 21$.

**3**. Find the area of this triangle



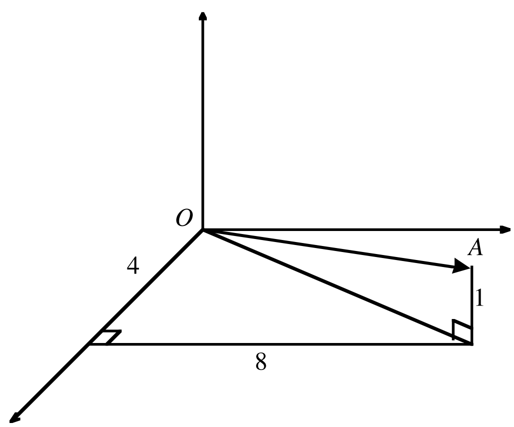

A $(13, 14, 15)$ triangle

Want another? Find the area of the triangle whose sides have length $91, 222, 205$.

**4.** How long is $\overrightarrow{OA}$?

What if $A = (14, 5, 2)$?

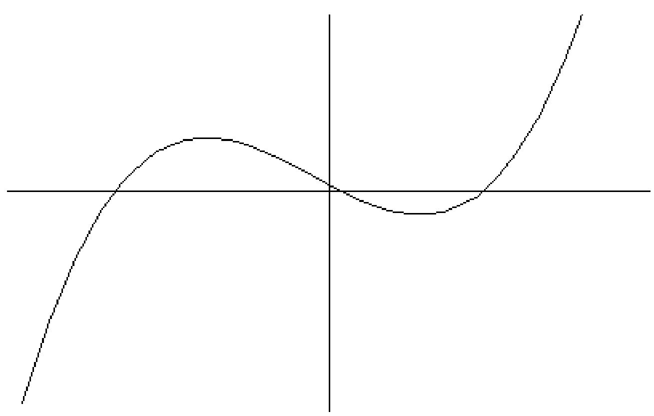
.




**5.** Suppose $f(x) = 140 - 144\,x + 3\,x^2 + x^3$. Find the zeros, extrema, and inflection points for the graph of $f$.

There's more where this comes from. Try

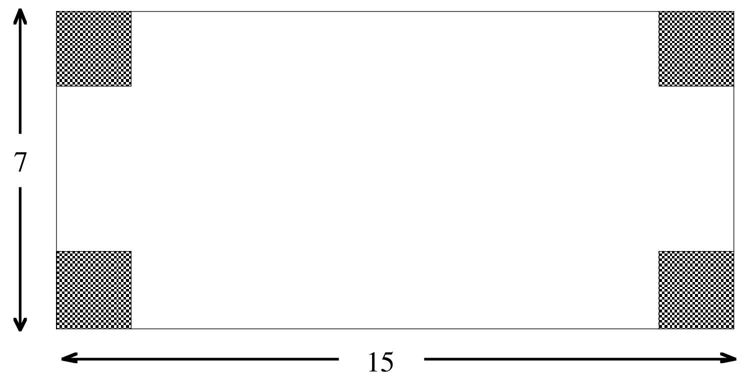
$f(x) = -175 - 45\,x + 3\,x^2 + x^3$



$f(x) = 140 - 144\,x + 3\,x^2 + x^3$

**6**. What size cut-out maximizes the volume?

Or, suppose the box measured, say, $9 \times 24$.




## Getting Started

One of the most famous and useful results from Euclidean geometry is the Pythagorean theorem:

**Theorem 1**

*If a right triangle has legs of length a and b and if its hypotenuse has length c, then*

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

The Greek geometers had a much more geometric way of saying this: *The square upon the hypotenuse is equal to the squares upon the legs*. Draw a picture of what they were talking about.

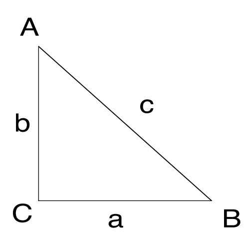



Figure 1

**7**. Describe your favorite proof of the Pythagorean Theorem.

After stating (and perhaps proving) the Pythagorean theorem, most geometry texts contain a few exercises that ask students to "solve" right triangles (given two of the three sides, find the third). Sometimes, the solutions are "nice"—the side lengths are all integers. The most famous such *Pythagorean triple* is $(3, 4, 5)$. Of course, a right triangle need not have integers for side lengths; if the legs have length 1 and 2, the hypotenuse has length $\sqrt{5}$.

The converse of the Pythagorean theorem is also true (proof?) and surveyors from antiquity knew that if a triangle has sides in the ratio of $3 : 4 : 5$, it has to be a right triangle.

One of the oldest "task design" problems is surely the problem of finding Pythagorean triples.

**8**. What's your favorite way to generate Pythagorean triples?

# 1 An algebraic approach

## How to Amaze Your Friends at Parties

A *Gaussian Integer* is a complex number of the form $a + bi$ where $a$ and $b$ are *integers*.

Example: $3 + 2i$. Non-example: $\frac{1}{2} + i\sqrt{2}$.

Remember from last summer? The system of Gaussian integers is denoted by $\mathbb{Z}[i]$. $\mathbb{Z}[i]$ has the UFP. What are the units?

**FOR DISCUSSION**

Pick your favorite Gaussian Integer (make $a > b$) **and square it**.

## Why does this work?

Finding Pythagorean triples amounts to finding triples of integers $(a, b, c)$ so that $a^2 + b^2 = c^2$. If you are "thinking Gaussian integers," the form $a^2 + b^2$ should look familiar. It is the *norm* of the Gaussian integer $a + bi$. Just to refresh your memory, here are the relevant definitions and properties:

**All you ever wanted to know about conjugation and Norm.**

... but were afraid to ask.

1. If $z = a + bi$ is a Gaussian integer, the "complex conjugate" of $z$, written $\overline{z}$, is defined by $\overline{z} = a - bi$
2. Using this definition, the following properties of conjugation hold:
   (a) $\overline{z + w} = \overline{z} + \overline{w}$ for all Gaussian integers $z$ and $w$.

(b) $\overline{zw} = \overline{z}\,\overline{w}$ for all Gaussian integers $z$ and $w$.
(c) $z = \overline{z} \Leftrightarrow z \in \mathbb{R}$
(d) $z\,\overline{z} = a^2 + b^2$, a non-negative integer.

3. The norm of $z$, written $N(z)$ is defined as the product of $z$ and its complex conjugate: $N(z) = z\,\overline{z}$.
4. Using this definition, the following properties of norm hold:

(a) $N(zw) = N(z)\,N(w)$ for all Gaussian integers $z$ and $w$.
(b) $N(z) = a^2 + b^2$, a non-negative integer.

Most of these statements make sense for general complex numbers, not just Gaussian integers. In fact, we can say that $\mathbb{Z}[i]$ "inherits" these properties from $\mathbb{C}$.

Property 4a is often described by saying "the norm is multiplicative." Norm is also the name of the guy on Cheers, but he wasn't multiplicative.

**1**. Prove properties 2 and 4 above.

**2**. Show that if $z$ is a Gaussian integer, then

$$N(z^2) = (N(z))^2$$

Notice that the right side of this equation is a *perfect square* (it is the square of an integer).

These properties show how taking conjugates and norms behave with respect to the binary operations in $\mathbb{Z}[i]$ and hence allow you to develop rules for calculating with conjugates and norms.

Problem 2 is a key to one of the nicest ways around for generating Pythagorean triples. The idea goes like this:

We'll look at another nice way in the next section.

### How to generate Pythagorean triples

- The equation $a^2 + b^2 = c^2$ can be written $N(z) = c^2$ where $z = a + bi$. So, we are looking for Gaussian integers whose norms are perfect squares.
- Problem 2 says that the norm of a Gaussian integer will be a perfect square if the Gaussian integer is itself a perfect square.
- So, to generate Pythagorean triples, pick a Gaussian integer at random, and square it. The square will be a Gaussian integer $a + bi$ whose norm, $a^2 + b^2$ will be a perfect square. That is, $a^2 + b^2$ will equal $c^2$ for some integer $c$, and $(a, b, c)$ will be a Pythagorean triple.

**3**. Generate half a dozen Pythagorean triples in this way.

**4**. Use the method to establish the following identity that is often used for generating Pythagorean triples:

$$(r^2 + s^2)^2 = (r^2 - s^2)^2 + (2rs)^2$$

If your kids don't know about Gaussian integers, you could simply ask them to prove the identity in problem 4—a nice exercise in algebra. But, of course, that masks where it comes from in the first place. The best thing to do is to show your class the Gaussian integers. Everyone should know about it.

**Write and Reflect:**

**5**. So, you can use norms of Gaussian integers to generate Pythagorean triples. Explain carefully what properties of the norm makes this technique work. That is, think of the norm as a function $N : \mathbb{Z}[i] \rightarrow \mathbb{Z}$. What properties of this function are essential to our method for generating Pythagorean triples?

This is an important question if you want to see how much of this technique leads to a general method and how much is just a happy accident.

**Take it Further.** There are some details that need to be taken care of:

**6**. This method produces duplicates, and sometimes produces negative "legs." Refine the algorithm so that it produces only positive triples and produces no duplicates.

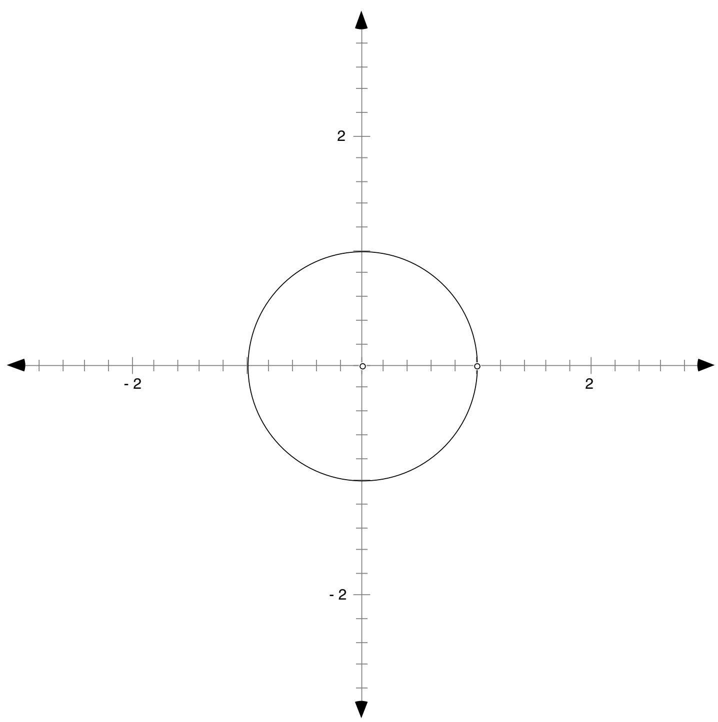
Hint: If $N(z) = N(w)$, what do you know about $z$ and $w$?

**7**. Even after you eliminate duplicates, there are annoying triples like $(6, 8, 10)$ that show up and are simple multiples of a "primitive" triple (this one is twice $(3, 4, 5)$). Characterize those $z$ so that $z^2$ will generate a *primitive* Pythagorean triple.

**8**. Use the unique factorization of $\mathbb{Z}[i]$ to show that this method of squaring and taking norms gives *all* Pythagorean triples.

# 2 A geometric approach

There is another way to generate Pythagorean triples, using the unit circle and coordinate geometry.



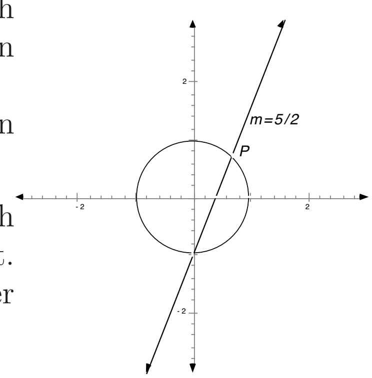

The unit circle

**1**. What is the equation of the unit circle?

**2**. (a) In the picture in the margin, the line passes through $(0, -1)$ and has slope $\frac{5}{2}$. What is its other intersection with the unit circle?

(b) Use the coordinates of $P$ to obtain a Pythagorean triple.




**3**. Pick another line with rational slope that passes through $(0, -1)$ and intersects the unit circle in the first quadrant. Use this second intersection point to determine another Pythagorean triple.

**4**. Prove the following theorem:

**Theorem 2**

*If a line passes through the point $(0, -1)$ and has rational slope and intersects the unit circle in two points, then its other intersection with the unit circle will be a rational point.*

"Rational point" means a point whose coordinates are rational numbers.

**5**. Suppose you had a rational point $P$ on the unit circle in the first quadrant. That is, $P = (\frac{a}{d}, \frac{b}{e})$. Use $P$ to find a Pythagorean triple.

Why do we want the point to be in the first quadrant?

**6**. What slopes for the line in theorem 2 should you use to get "second" intersection points in the first quadrant?

**7**. Use theorem 2 to generate several Pythagorean triples. Will this generate all of them or does it miss some? How do you know?

**8**. Suppose a line with slope $m$ intersects the unit circle at $(0, -1)$ and at $P$.

(a) Find the coordinates of $P$ in terms of $m$.

(b) Suppose $m$ is rational, say $m = \frac{r}{s}$. Express the Pythagorean triple you get from $P$ in terms of $r$ and $s$.

This is sometimes called a "parametrization" of the unit circle in terms of $m$. Why?

Compare with the result of problem 4 on page 7.

# 3 *The Norm Idea: Related Problems*

The problem of finding Pythagorean triples asks for integer sided triangles with a right angle. A natural generalization is to ask for integer sided triangles with some *other* kind of angle. For example, are there any triangles with integer side lengths and a $60^\circ$ angle?

Well, there are equilateral triangles, but how about scalene ones? These certainly exist—look at problem 2 on page 2. We're about to figure out how to find them.

Suppose there were.

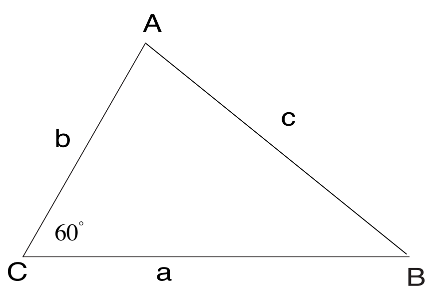



Figure 2: Integer side lengths, $m\angle C = 60^\circ$

In the case of a right triangle, the Pythagorean theorem gave us a relationship among the three sides ($a^2 + b^2 = c^2$). In a triangle where $\angle C$ is not a right angle, $a^2 + b^2$ is *not* the same as $c^2$, but there is a theorem that generalizes Pythagoras and tells us how the sides are related:

**Theorem 3**

***The law of cosines*** *If the sides of a triangle are labeled as in figure 3*

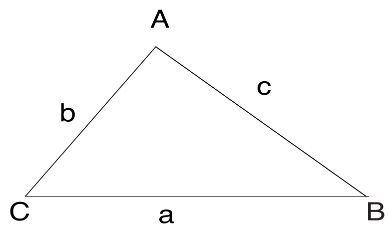



Figure 3

*then* $c^2 = a^2 + b^2 - 2ab\cos C$.

*Here, "C" means the measure of $\angle BCA$.*

**1**. Describe your favorite proof of the Law of Cosines.

**2**. In what sense is the law of cosines a generalization of the Pythagorean theorem?

There are many proofs of the law of cosines that are appropriate for second year algebra students. Try to find one that you could use in a *geometry* class.

So, let's go back to figure 2:

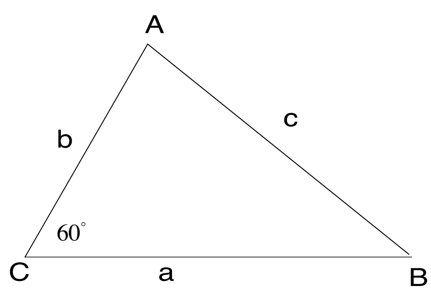



Figure 2: Integer side lengths, $m\angle C = 60°$

By the law of cosines,

$$\begin{aligned} c^2 &= a^2 + b^2 - 2ab\cos 60° \\ &= a^2 + b^2 - 2ab \cdot \tfrac{1}{2} \\ &= a^2 + b^2 - ab \end{aligned}$$

So, finding the kind of triangles we want amounts to finding triples of integers $(a, b, c)$ so that $a^2 - ab + b^2 = c^2$. Just as before, we are looking for $a, b \in \mathbb{Z}$ so that $a^2 - ab + b^2$ is a perfect square.

Well, there is another number system that you met last summer, that has a structure very similar to $\mathbb{Z}[i]$, and that has a norm function that will do the trick for us. Here's how it works. Suppose that

$$\omega = \frac{-1 + i\sqrt{3}}{2}$$

$\omega$ is a root of the equation $x^2 + x + 1 = 0$. We can construct the subring of the complex numbers

How would one even know to look at $\mathbb{Z}[\omega]$? Good question. See the appendix on page 22. Notice that $i^4 = 1$ and $\omega^3 = 1$, so $i$ and $\omega$ are both "roots of unity."

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$

Since $\omega^2 + \omega + 1 = 0$,

$$\omega^2 = -1 - \omega$$

so you can calculate like this:

- You add the elements in the usual way:

$$(3 + 4\omega) + (5 + 7\omega) = 8 + 11\omega$$

- You multiply the elements in the usual way and then replace $\omega^2$ by $-1 - \omega$.

$$\begin{aligned} (3 + 4\omega)(5 + 7\omega) &= 15 + 41\omega + 28\omega^2 \\ &= 15 + 41\omega + 28(-1 - \omega) \\ &= -13 + 13\omega \end{aligned}$$

This shows that $\mathbb{Z}[\omega]$ is closed under addition and multiplication.

**3**. Show that
(a) $\omega^2 = \overline{\omega}$
(b) $\omega^3 = 1$
(c) $(a + b\omega)(a + b\overline{\omega}) = a^2 - ab + b^2$

Problem 3c is our ticket to the 60° triangle problem. Note that

Justify each step? Try it.

$$\begin{aligned} N(a + b\omega) &= (a + b\omega)\left(\overline{a + b\omega}\right) \\ &= (a + b\omega)\left(\overline{a} + \overline{b\omega}\right) \\ &= (a + b\omega)\left(\overline{a} + \overline{b}\,\overline{\omega}\right) \\ &= (a + b\omega)\left(a + b\,\overline{\omega}\right) \\ &= a^2 - ab + b^2 \end{aligned}$$

So, the thing we want to make a perfect square is the norm of one of these funny new numbers. But the norm is still multiplicative, so, to make the norm a square, make the *thing* a square.

The norm is still multiplicative, becuase it is multiplicative on all of $\mathbb{C}$. It is multiplicative on all of $\mathbb{C}$ because it is defined by $N(Z) = z\overline{z}$ (see problem 4 on page 7).

## EXAMPLE

Start with $z = 3 + 2\omega$. Square it:

$$\begin{aligned} z^2 &= (3+2\omega)^2 \\ &= 9 + 12\omega + 4\omega^2 \\ &= 9 + 12\omega + 4(-1-\omega) \quad \text{(Don't forget: } \omega^2 = -1-\omega) \\ &= 5 + 8\omega \end{aligned}$$

So, arguing as before,

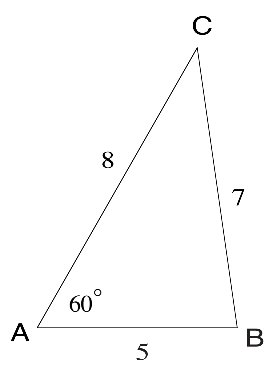
$$\begin{aligned} 5^2 - 8\cdot 5 + 8^2 &= N(5+8\omega) \\ &= N\left((3+2\omega)^2\right) \\ &= \left(N(3+2\omega)\right)^2 \\ &= 7^2 \end{aligned}$$

and voilà:

$$5^2 - 5\cdot 8 + 8^2 = 49 \quad \text{a perfect square!}$$

So the triangle whose sides have length 5, 8, and 7 has a 60° angle.

Or, a triangle with sides of length 5 and 8 and an included angle of 60° has a third side of length 7.




A $(5, 8, 7)$ triangle has a 60° angle

**Historical Perspective**

We like to call triples of integers $(a, b, c)$ *Eisenstein triples* if

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

George Eisenstein, a student of Gauss, was very fond of the ring $\mathbb{Z}[\omega]$.

Eisenstein also devised a beautiful proof of quadratic reciprocity (the one used in PROMYS). When asked to name the three greatest mathematicians of all time, Gauss replied "Archimedes, Newton, and Eisenstein." It was one of the few times in his life when Gauss was wrong. The correct answer is, of course, "Archimedes, Newton, and Gauss."

Remember: $\omega^3 = 1$. Eisenstein was very interested in roots of the equation $x^n - 1$ where $n \in \mathbb{Z}^+$.

**4**. Find three other triangles with one 60° angle and integer sidelengths. Are there infinitely many such triangles? Prove it.

**5**. Use the method of norms to establish the following identity that is often used for generating Eisenstein triples:

$$(r^2-s^2)^2-(r^2-s^2)(2rs-s^2)+(2rs-s^2)^2 = (r^2-r\ s+s^2)^2$$

If your kids don't know about $\mathbb{Z}[\omega]$, you could simply ask them to prove this identity—a nice exercise in algebra. But, of course, that masks where it comes from in the first place. The best thing to do is to show your class $\mathbb{Z}[\omega]$. Everyone should know about it.

**Take It Further**

**6**. Will this method generate all Eisenstein triples?

Hint: $\mathbb{Z}[\omega]$ has the UFP, but there are six units. Remember what they are?

**7**. Find a triangle whose sides have integral length and so that one angle has a cosine of $\frac{3}{5}$. Are there infinitely many such triangles? Prove it.

**8**. Can you find a triangle with a 45° angle and integer sidelengths? Try the same method, and find three such triangles or explain what goes wrong.

**9**. Under what conditions on $\theta$ will a method like this allow you to generate integer-sided triangles with one angle measuring $\theta$?

# 4 The Intersection Idea: Related Problems

When you wanted to find triples where $a^2 + b^2 = c^2$, you used the graph of $x^2+y^2 = 1$ (the unit circle) to generate them. Now look back at the problem of finding triangles with integer sides and one 60° angle. You want triples where $a^2 - ab + b^2 = c^2$. Could you use a similar geometric approach to generate them?

**1**. If you have a rational point on the graph of $x^2-xy+y^2 = 1$, can you use it to find the integer-sided triangle you are looking for? Prove it.

**2**. Graph $x^2 - xy + y^2 = 1$. What kind of object is it?

**3**. Prove the following theorem:

We think the proof of this theorem involves a great deal of "reasoning about calculations." Do you?

**Theorem 4**

*If a line passes through the point* $(0, -1)$*, has rational slope, and intersects the graph of* $x^2 - xy + y^2 = 1$ *in two points, then its other intersection will be a rational point.*

**4**. Use theorem 4 to find several triangles with one 60° angle and integer sidelengths.

**5**. Suppose a line with slope $m$ intersects the curve with equation $x^2 - xy + y^2 = 1$ at $(0, -1)$ and at $P$.
(a) Find the coordinates of $P$ in terms of $m$.
(b) Suppose $m$ is rational, say $m = \frac{r}{s}$. Express the Eisenstein triple you get from $P$ in terms of $r$ and $s$.

This is sometimes called a "parametrization" of the ellipse in terms of $m$. Why?

Compare with the result of problem 5 on page 15.

**Take It Further**

**6**. Use this method to find a triangle whose sides have integral length and so that one angle has a cosine of $\frac{3}{5}$. Are there infinitely many such triangles? Prove it.

**7**. Can you use this method to find a triangle with a $45°$ angle and integer sidelengths? Try it, and find three such triangles or explain what goes wrong.

**8**. The problem of finding a triangle with integer sides and one angle $\theta$ comes down to finding the right conic section $C$. Express the equation of $C$ in terms of $\theta$ and give a condition that $\theta$ and $C$ have to meet in order for this problem to have a solution.

---

**Write and Reflect:**

**9**. Compare the "norm equation" and the "secant and conic" method for finding integer sided triangles with prescribed angles. Are they equivalent?

---

# 5 *What's Your Favorite Task-design Problem?*

So, that's the story for today. The two methods—norms from appropriate number systems and finding rational points on conics—are two general-purpose methods for building nice problems for a wide array of middle and high school topics.

Try out one of these methods, or anything else you want to use, on a task-design problem of your own.

**PROBLEM**

Describe a task-design problem you've wondered about in your teaching. Use the norm or conic method (or anything else) to solve it.

**For your enjoyment.** Just in case you need some inspiration, here are some examples.

Stop! Don't read the examples until you've thought about a problem of your own.

**1**. (From calculus.) Every calculus course has box problems:

> A rectangle measures $7 \times 15$. Little squares are cut out of the corners, and the sides are folded up to make a box. Find the size of the cut-out that maximizes the volume of the box.

The *real* box problem is this:

> A rectangle measures $a \times b$. Little squares are cut out of the corners, and the sides are folded up to make a box. Find a method to generate $a$ and $b$ if we insist that the size of the cut-out that maximizes the volume of the box is a rational number.

Use today's methods to solve the real box problem.

**2**. (From geometry.) Pythagorean triples can be used to find a lattice points in the plane that is an integer distance away from the origin (how?). Find some lattice points in $\mathbb{Z}^3$ that are integer distances away from the origin.

**3**. (From algebra 1.) Bowen Kerins and David Offner (two illustrious PROMYS alumns) taught a 3-week course for high school teachers at PCMI last summer. The course was entitled "Applications of Gaussian Integers and Related Systems to Secondary Teaching." The teachers at PCMI worked on several task-design problems. One of them is described by Bowen like this:

> The group also focused on a few standard types of problems seen in algebra; in particular, the group found an excellent method to generate problems collectively known as "current" or "wind" problems like this one:
>
> > A boat is making a round trip, 135 miles in each direction. Without a current, the boat's speed would be 32 miles per hour. However, there is a constant current that increases the boat's speed in one direction and decreases it in the other. If the round trip takes exactly 9 hours, what is the speed of the current?

Notice that the answer to this problem is something like "8," not "$\frac{3+\sqrt{37}}{2}$." How'd they do that?

The course was designed by Bowen, Ryota, David, Michelle, and Tanya.

**4**. (From geometry.) Heron's formula shows how to find the area of a triangle in terms of the lengths of its sides. A "Heron triangle" is a triangle with integer sidelengths and integer area. Use the methods of this section to find some Heron triangles.

Heron: If the sidelengths of a triangle are $a$, $b$, and $c$, its area is $\frac{1}{2}\sqrt{s(s-a)(s-b)(s-c)}$ where $s$ is half the perimeter. Proof?

**5**. (From analytic geometry.) Find three points $A$, $B$, and $C$ in the plane so that

- the coordinates of $A$, $B$, and $C$ are integers and
- the distance between any two of the three points is an integer.

The identity

$$(r^2+s^2)^2 = (r^2-s^2)^2+(2rs)^2$$

from page 7 holds in any commutative ring.

**6**. (From precalculus.) How do you generate cubic polynomial functions with integral coefficients, with three rational zeros, two rational extrema, and one rational inflection point? No cheating: the six rational points must all be distinct.

**Hints:**
Let's handle a special case of the "depressed" monic cubic

$$f(x) = x^3 + cx + d$$

This setup insures that $f''$ has a rational root (namely 0). $f'$ will have rational roots if we put $c = -3q^2$ for some integer $q$. So, now our function is

$$f(x) = x^3 - 3q^2x + d$$

If $f$ has two rational roots, it has three (because the product of all three roots is rational), so it's enough to make two roots, say, $-\alpha$ and $\beta$, rational. But if $f(-\alpha) = f(\beta) = 0$, we have

$$-\alpha^3 + 3q^2\alpha = \beta^3 - 3q^2\beta$$

or

$$\beta^3 + \alpha^3 = 3q^2(\alpha + \beta)$$

Since $\alpha + \beta \neq 0$ (we want our roots distinct), this is the same as

$$\alpha^2 - \alpha\beta + \beta^2 = 3q^2$$

or

$$N(\alpha + \beta\omega) = 3q^2$$

where $\omega = \frac{-1+i\sqrt{3}}{2}$. Look familiar now?

"Monic" means that the leading coefficient is 1. "Depressed" means that the coefficient of $x^2$ is 0 (maybe the cubic feels depressed because it's missing a term). Given any monic cubic, $x^3 + bx^2 + cx + d$, replacing $x$ by $x - \frac{b}{3}$ will depress it (this translates the graph to a symmetry point), so this isn't really a serious constraint.

**Take it Further** A *congruent* number is an integer $n$ such that there is a right triangle with rational sidelengths and area $n$.

Notice that the sides in the right triangle need only be rational (not integral). So, the area of any triangle whose sides form a Pythagorean triple is a congruent number, but not all congruent numbers are obtained this way. For example, 157 is a congruent number, because the (right) triangle whose sides are

$$\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830},$$

$$\frac{6803294847826435051217540}{411340519227716149383203}, \quad \text{and}$$

The calculations here were made by Don Zagier. How in the world do you think he did it?

$$\frac{411340519227716149383203}{21666555693714761309610}$$

has area 157.

**7**. Show that 5 and 6 are congruent numbers but that 4 is not.

**8**. Show that n is a congruent number if and only if there exists a rational number $x$ so that $x^2 + n$ and $x^2 - n$ are squares of rational numbers.

**9**. Find a way to generate congruent numbers.

The fact that 4 is not a congruent number can be used to show that there are no integers $(x, y, z)$ all non-zero such that $x^4 + y^4 = z^4$, a special case of Fermat's last theorem.

Determining all congruent numbers is an unsolved problem. In the middle of the last (20th) century, Heegner (a high school teacher in Germany) applied powerful techniques from analytic number theory to the congruent number problem, setting a new direction for research on the topic. A detailed account of what is known is in the book *Introduction to Elliptic Curves and Modular Forms* by Neal Koblitz (Springer-Verlag, 1993).

# Appendix: What if you didn't know about Eisenstein integers?

Suppose we were working on the 60° problem, and we wanted to employ the norm idea, but we didn't know about $\omega$. How in the world would someone know that the right system to use is $\mathbb{Z}[\omega]$. Through some wishful thinking. Here's how:

If $a^2-ab+b^2$ were the "norm" of something, and if that norm function behaved like the ordinary norm from the Gaussian integers (in particular, if the norm of a product were the product of the norms), then we'd be able to use the same method: Take a thing, square it, and then its norm would

- have the right form $(a^2 - ab + b^2)$ and
- be a perfect square.

Well, this is not the norm of $a + bi$, but suppose it were the norm of $a + b\omega$ for some complex number $\omega$. Let's work backwards and see if we could figure out what $\omega$ would have to be. Remember, the norm is the product of the number and its conjugate, so, if $a$ and $b$ are integers,

$$\begin{aligned} N(a+b\omega) &= (a+b\omega)\left(\overline{a+b\omega}\right) \\ &= (a+b\omega)\left(\overline{a}+\overline{b\omega}\right) \\ &= (a+b\omega)\left(\overline{a}+\overline{b}\,\overline{\omega}\right) \\ &= (a+b\omega)\left(a+b\,\overline{\omega}\right) \\ &= a^2+ab(\omega+\overline{\omega})+b^2(\omega\,\overline{\omega}) \end{aligned}$$

and if we want this to be $a^2 - ab + b^2$, then we want

As usual, justify each step in the above calculation.

$$\begin{aligned} \omega+\overline{\omega} &= -1 \quad \text{and} \\ \omega\,\overline{\omega} &= 1 \end{aligned}$$

Well, that pretty much nails $\omega$ down: we know the sum of $\omega$ and its complex conjugate (it's $-1$) and we know the product $\omega\,\overline{\omega}$ (it's 1). So, $\omega$ is a root of the quadratic equation

$$x^2 + x + 1 = 0$$

This is because of the old chant from high school:

$$x^2 - (\text{the sum of the roots})\, x + (\text{the product of the roots}) = 0$$

Using the quadratic formula, we can take $\omega$ to be

$$\omega = \frac{-1 + i\sqrt{3}}{2}$$

and we can now generate as many triples of integers $(a, b, c)$ so that $c^2 = a^2 - ab + b^2$ as we like.

The other root is then $\overline{\omega} = \frac{-1-i\sqrt{3}}{2}$. That will work, too.

## References

N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer Verlag, New York, 1993

A. Cuoco, "Meta-Problems in Mathematics," *College Mathematics Journal*, November, 2000.

EDC, "Pythagorans and Cousins," in *Connecting with Mathematics*, Corwin Press (in press).

B.Kerins (and a supporting cast of 50), "Gauss, Pythagoras, and Heron," to appear in the new column *Delving Deeper* in the *Mathematics Teacher*, May 2003.