Challenge: Expand

$$(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)\cdots.$$

After some work, we collaboratively came up with the following:

$$(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)\cdots = 1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-x^{35}-x^{40}+x^{51}+x^{57}-\cdots.$$

What's the pattern? The sign pattern is clear: we have

$$\prod_{k\geq 1}(1-x^k) = 1+\sum_{n\geq 1}(-1)^n(x^{P_n}+x^{P'_n}).$$

But what can we say about the mysterious sequences P_n and P'_n? Kimberly observed that $P_n - P'_n = n$ for all n; this reduces the problem to figuring out P_n.

Euler's Pentagonal Number Theorem. The above product holds with P_n being the sequence of *pentagonal numbers*.

Before explaining exactly what the pentagonal numbers are, we warm up with a couple of other sequences:

(1) The *triangular numbers.*

The triangular numbers are defined

$$T_1 := 1 \qquad T_2 := 3 \qquad T_3 := 6 \qquad T_4 := 10 \qquad \cdots$$

The illustration below[1] should make clear where the name comes from:

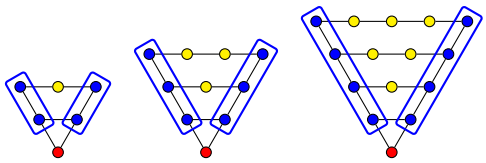

Illustration of T_3, T_4, and T_5

More generally,

$$T_n = \sum_{1\leq k\leq n} k = \frac{n(n+1)}{2}$$

(2) The *square numbers.*

The square numbers are defined $1, 4, 9, 16, \ldots$ Here's a picture:

[1] Tex code used to draw this thanks to an amazing post by user *Qrrbrbirlbel* on `tex stackexchange`.

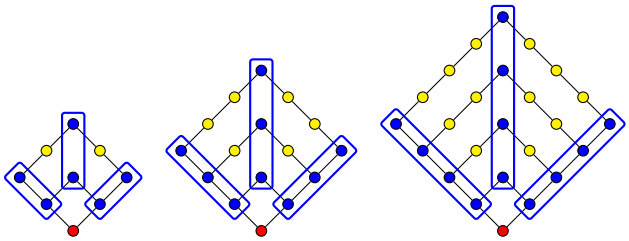

Illustration of square numbers

(3) The *pentagonal numbers.*

The pentagonal numbers are defined

$$P_1 := 1 \qquad P_2 := 5 \qquad P_3 := 12 \qquad P_4 := 22 \qquad \cdots$$

It's clear that P_1 can be represented by a single point and P_2 by a pentagon, but what about P_3 onwards? After some consideration, Max proposed the following:

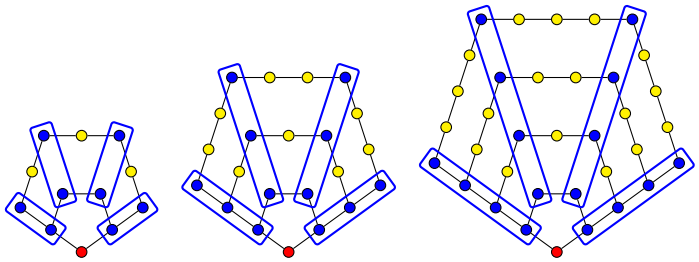

Illustration of P_3, P_4, and P_5

How do we get a formula for P_n? Ben pointed out that the second rate of change is constant (namely, 3). Thus the first rate of change is like $3n$ ($+C$, as we remember from calculus!), so the function P_n should grow like $\frac{3}{2}n^2$. By comparing this with the actual values of P_n, we quickly deduced that

$$P_n = \frac{n(3n-1)}{2}$$

(An alternative is to carefully examine the color-coding in the pictures above.) With P_n in hand, we can easily compute $P'_n = P_n + n = \frac{n(3n+1)}{2}$.

Sums of polygonal numbers. Having warmed up with polygonal numbers, we now return to the familiar

Lagrange's Four-Squares Theorem: Every n is the sum of four squares.

Long before this was proved, a remarkable generalization had been formulated (by Girard, and subsequently by Fermat):

Fermat's Polygonal Numbers Conjecture: Every $n \geq 1$ is the sum of 3 triangular numbers, 4 squares, 5 pentagonal numbers, and (more generally) k many k-gonal numbers.

As you might imagine, this conjecture isn't so easy to prove. After Lagrange's success with squares, the next step is due to Gauss:

Gauss' Eureka Theorem: $n = \triangle + \triangle + \triangle$.

The entire polygonal conjecture was proved by Cauchy soon thereafter. Although we won't cover the proof of this in our course, it is accessible to you (in the sense that it doesn't require any tools you haven't already learned), and I encourage you to read up on it. From here, we explore our final question about sums of squares, which also happens to be a natural segue into our last main topic in the course: elliptic curves.

PYTHAGOREAN TRIPLES:

Challenge: Find all integer solutions to

$$x^2 + y^2 = z^2. \qquad (\spadesuit)$$

Any integer solution $(x, y, z) \in \mathbb{Z}^3$ is called a *pythagorean triple* because, as Konnor pointed out, this is equivalent to asking about right triangles with integer sides. (Some history: Plimpton 322 is an ancient Babylonian tablet with what appear to be a list of enormous pythagorean triples. This problem was more carefully considered in Euclid's classic book, *The Elements*.)

Notation: From now on we'll abbreviate *pythagorean triple* as PT.

What are some PTs? Right away we can generate infinitely many trivial solutions to $(\spadesuit)$:

$$(x, y, z) = (0, \pm a, \pm a) \quad \text{or} \quad (\pm a, 0 \pm a).$$

This isn't too interesting. Are there any nontrivial PTs (x, y, z)? Sure:

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

Are there infinitely many nontrivial pythagorean triples? Yes! Just take all scalar multiples of $(3, 4, 5)$:

$$(3, 4, 5), (6, 8, 10), (9, 12, 15), \ldots$$

This feels like cheating, though. The real question is, are there infinitely many legitimately different PTs? Let's call those triples that aren't multiples of other triples *primitive*. The

rest – the PTs that are multiples of other PTs – we call *imprimitive*. We can describe the primitive PTs in a different way:

Proposition (Miranda): A pythagorean triple (a, b, c) is *primitive* if and only if $(a, b) = 1$.
Proof.
($\Leftarrow$) Straightforward.
($\Rightarrow$) Suppose $(a, b) > 1$. Then $\exists p \mid (a, b)$. Since $a^2 + b^2 = c^2$, we deduce

$$p \mid a^2 + b^2 \implies p \mid c^2 \implies p \mid c.$$

But then $(\frac{a}{p}, \frac{b}{p}, \frac{c}{p})$ is also a PT, whence (a, b, c) isn't primitive. □

We thus arrive at a refinement of our original challenge:

Challenge v2.0: Find all nontrivial primitive pythagorean triples.

We will solve this using geometry. The key insight is that if (a, b, c) is a PT, then $\left(\frac{a}{c}, \frac{b}{c}\right)$ is a point on the unit circle. Conversely, if we have any point (α, β) on the unit circle with both $\alpha, \beta \in \mathbb{Q}$, this produces a PT. This motivates the following definition:

Definition: A *rational point* is any element of $\mathbb{Q}^2$, i.e. any coordinate pair (x, y) with $x, y \in \mathbb{Q}$.

Thus, to find all PTs it suffices to find all rational points on the unit circle. We'll solve this problem next time.