The secret lives of polynomial identities

Bruce Reznick
University of Illinois at Urbana-Champaign

University of Konstanz
June 30, 2011

"An idea which can be used only once is a trick. If you can use it more than once it becomes a method." – George Pólya and Gábor Szegö

"An idea which can be used only once is a trick. If you can use it more than once it becomes a method." – George Pólya and Gábor Szegö

Mathematics is the art of logic and formulas are its poetry.

"An idea which can be used only once is a trick. If you can use it more than once it becomes a method." – George Pólya and Gábor Szegö

Mathematics is the art of logic and formulas are its poetry.

I have always been fascinated by exact formulas, especially finite ones such as polynomial identities.

"An idea which can be used only once is a trick. If you can use it more than once it becomes a method." – George Pólya and Gábor Szegö

Mathematics is the art of logic and formulas are its poetry.

I have always been fascinated by exact formulas, especially finite ones such as polynomial identities.

They can seem easy and superficial, but the fact that they are true without hypotheses can make mathematicians uncomfortable.

"An idea which can be used only once is a trick. If you can use it more than once it becomes a method." – George Pólya and Gábor Szegö

Mathematics is the art of logic and formulas are its poetry.

I have always been fascinated by exact formulas, especially finite ones such as polynomial identities.

They can seem easy and superficial, but the fact that they are true without hypotheses can make mathematicians uncomfortable.

They don't **need** us.

“An idea which can be used only once is a trick. If you can use it more than once it becomes a method.” – George Pólya and Gábor Szegö

Mathematics is the art of logic and formulas are its poetry.

I have always been fascinated by exact formulas, especially finite ones such as polynomial identities.

They can seem easy and superficial, but the fact that they are true without hypotheses can make mathematicians uncomfortable.

They don’t **need** us.

They come into view unexpectedly, like meteorites on a vast Arctic plain. Once we see them and stare at them long enough, we find that the best identities can signify deep and distant phenomena.

The two square identity is widely used in algebra and number theory:

$$(a^2 + b^2)(x^2 + y^2) = (ax - by)^2 + (bx + ay)^2$$

The two square identity is widely used in algebra and number theory:

$$(a^2 + b^2)(x^2 + y^2) = (ax - by)^2 + (bx + ay)^2$$

It can be derived by using the commutative and associative law for complex numbers:

$$\Big((a + ib)(a - ib)\Big)\Big((x + iy)(x - iy)\Big)$$

$$\Big((ax - by) + i(bx + ay)\Big)\Big((ax - by) - i(bx + ay)\Big)$$
$$= \Big((a + ib)(x + iy)\Big)\Big((a - ib)(x - iy)\Big),$$

The two square identity is widely used in algebra and number theory:

$$(a^2 + b^2)(x^2 + y^2) = (ax - by)^2 + (bx + ay)^2$$

It can be derived by using the commutative and associative law for complex numbers:

$$\Big((a + ib)(a - ib)\Big)\Big((x + iy)(x - iy)\Big)$$

$$\Big((ax - by) + i(bx + ay)\Big)\Big((ax - by) - i(bx + ay)\Big)$$
$$= \Big((a + ib)(x + iy)\Big)\Big((a - ib)(x - iy)\Big),$$

And by setting $(a, b) = (\cos t, \sin t)$, it shows that distance is invariant under a rotation of axes.

The two square identity is widely used in algebra and number theory:

$$(a^2 + b^2)(x^2 + y^2) = (ax - by)^2 + (bx + ay)^2$$

It can be derived by using the commutative and associative law for complex numbers:

$$\Big((a + ib)(a - ib)\Big)\Big((x + iy)(x - iy)\Big)$$

$$\Big((ax - by) + i(bx + ay)\Big)\Big((ax - by) - i(bx + ay)\Big)$$
$$= \Big((a + ib)(x + iy)\Big)\Big((a - ib)(x - iy)\Big),$$

And by setting $(a, b) = (\cos t, \sin t)$, it shows that distance is invariant under a rotation of axes.

Not bad for one identity.

Not all identities are interesting, of course. Sometimes they're just a consequence of linear dependence. For example, who cares that

$$(x + 2y)^2 + (2x + 3y)^2 + (3x + 4y)^2 = 14x^2 + 40xy + 29y^2 \ ?$$

The left hand side has to equal ... *some* binary quadratic form. Of course, identities based on dependence can become interesting if their coefficients have additional properties.

Not all identities are interesting, of course. Sometimes they're just a consequence of linear dependence. For example, who cares that

$$(x + 2y)^2 + (2x + 3y)^2 + (3x + 4y)^2 = 14x^2 + 40xy + 29y^2 \text{ ?}$$

The left hand side has to equal ... *some* binary quadratic form. Of course, identities based on dependence can become interesting if their coefficients have additional properties.

For example, the binomial theorem and the formula for the n-th difference:

$$\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k = (x + y)^n$$

$$\sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} (x + ky)^n = n!\ y^n.$$

Not all identities are interesting, of course. Sometimes they're just a consequence of linear dependence. For example, who cares that

$$(x+2y)^2+(2x+3y)^2+(3x+4y)^2 = 14x^2+40xy+29y^2 \ ?$$

The left hand side has to equal ... *some* binary quadratic form. Of course, identities based on dependence can become interesting if their coefficients have additional properties.

For example, the binomial theorem and the formula for the n-th difference:

$$\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k = (x+y)^n$$

$$\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}(x+ky)^n = n!\ y^n.$$

Identities are also interesting if there are many fewer summands than you'd expect.

What do we demand from a “good” polynomial identity?

What do we demand from a “good” polynomial identity?

“Astonish me!” – Sergei Diaghilev to Jean Cocteau, on what he wanted in the libretto to the ballet “Parade”.

What do we demand from a “good” polynomial identity?

“Astonish me!” – Sergei Diaghilev to Jean Cocteau, on what he wanted in the libretto to the ballet “Parade”.

This talk consists of stories about some semi-astonishing identities: their deeper meanings and how they can (or maybe should) be derived.

The first identity must have its roots in 19th century mathematics, although in this explicit form, I've only been able to trace it back to the mid 1950s. It's one of a family, and it's not accidental in this version that $(1^2 + (\sqrt{3})^2)^5 = 2^{10} = 1024$:

$$1024x^{10} + 1024y^{10} + (x + \sqrt{3}\,y)^{10} + (x - \sqrt{3}\,y)^{10} + (\sqrt{3}\,x + y)^{10} + (\sqrt{3}\,x - y)^{10} = 1512(x^2 + y^2)^5 \tag{1}$$

The first identity must have its roots in 19th century mathematics, although in this explicit form, I've only been able to trace it back to the mid 1950s. It's one of a family, and it's not accidental in this version that $(1^2 + (\sqrt{3})^2)^5 = 2^{10} = 1024$:

$$\begin{aligned} 1024x^{10} + 1024y^{10} + (x + \sqrt{3}\ y)^{10} + (x - \sqrt{3}\ y)^{10} \\ +(\sqrt{3}\ x + y)^{10} + (\sqrt{3}\ x - y)^{10} = 1512(x^2 + y^2)^5 \end{aligned} \tag{1}$$

The story of (1) and (4) (a few slides from now) and their generalizations runs through at least number theory, numerical analysis, functional analysis and combinatorics.

The second identity is very old; it goes back to Viète:

$$x^3 + y^3 = \left(\frac{x^4 + 2xy^3}{x^3 - y^3}\right)^3 + \left(\frac{y^4 + 2x^3y}{y^3 - x^3}\right)^3, \qquad (2)$$

The second identity is very old; it goes back to Viète:

$$x^3 + y^3 = \left(\frac{x^4 + 2xy^3}{x^3 - y^3}\right)^3 + \left(\frac{y^4 + 2x^3y}{y^3 - x^3}\right)^3, \qquad (2)$$

This is used to show that a sum of two cubes of rational numbers can usually be so expressed in infinitely many ways. For example:

$$2^3 + 1^3 = \left(\frac{20}{7}\right)^3 + \left(-\frac{17}{7}\right)^3 = \left(-\frac{36520}{90391}\right)^3 + \left(\frac{188479}{90391}\right)^3 = \dots$$

The second identity is very old; it goes back to Viète:

$$x^3 + y^3 = \left(\frac{x^4 + 2xy^3}{x^3 - y^3} \right)^3 + \left(\frac{y^4 + 2x^3y}{y^3 - x^3} \right)^3, \qquad (2)$$

This is used to show that a sum of two cubes of rational numbers can usually be so expressed in infinitely many ways. For example:

$$2^3 + 1^3 = \left(\frac{20}{7} \right)^3 + \left(-\frac{17}{7} \right)^3 = \left(-\frac{36520}{90391} \right)^3 + \left(\frac{188479}{90391} \right)^3 = \dots$$

The story here is a description of all homogeneous solutions to

$$x^3 + y^3 = p^3(x, y) + q^3(x, y), \qquad p, q \in \mathbb{C}(x, y).$$

Viète's derivation of his identity, curiously, is formally identical to a common technique in the modern study of elliptic curves.

The third identity was independently found by Desboves (1880) and Elkies (1995):

$$(x^2 + \sqrt{2}\, x\, y - y^2)^5 + (i\, x^2 - \sqrt{2}\, x\, y + i\, y^2)^5 + (-x^2 + \sqrt{2}\, x\, y + y^2)^5 + (-i\, x^2 - \sqrt{2}\, x\, y - i\, y^2)^5 = 0. \tag{3}$$

The third identity was independently found by Desboves (1880) and Elkies (1995):

$$(x^2 + \sqrt{2}\,x\,y - y^2)^5 + (i\,x^2 - \sqrt{2}\,x\,y + i\,y^2)^5 + (-x^2 + \sqrt{2}\,x\,y + y^2)^5 + (-i\,x^2 - \sqrt{2}\,x\,y - i\,y^2)^5 = 0. \tag{3}$$

It was first discovered by observing that

$$\sum_{k=0}^{3}(i^k x^2 + i^{2k} a\,x\,y + i^{3k} y^2)^5 = 40a(a^2+2)(x^7y^3 + x^3y^7),$$

and then setting $a = \sqrt{-2}$ and $y \to i\,y$. But why $\sqrt{-2}$? The full story ultimately depends on Newton's Theorem on symmetric polynomials. Commutative algebra and algebraic geometry also play a role, but Felix Klein would say it's all based on the cube.

The fourth identity was used by Liouville to show that every positive integer is a sum of at most 53 4th powers of integers:

$$\sum_{1\le i<j\le 4} \left((x_i+x_j)^4+(x_i-x_j)^4\right) = 6(x_1^2+x_2^2+x_3^2+x_4^2)^2. \qquad (4)$$

The fourth identity was used by Liouville to show that every positive integer is a sum of at most 53 4th powers of integers:

$$\sum_{1 \le i < j \le 4} \left((x_i + x_j)^4 + (x_i - x_j)^4 \right) = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2. \qquad (4)$$

Many similar and more complicated formulas were found in the late 19th century, until Hilbert showed that they must exist in all degrees.

As one indication of their geometric and combinatorial significance, if you take the the coordinates of the coefficients of the $2\binom{4}{2}$ linear forms in this identity, together with their antipodes, you get the 24 points $(\pm 1, \pm 1, 0, 0)$ and their permutations.

The fourth identity was used by Liouville to show that every positive integer is a sum of at most 53 4th powers of integers:

$$\sum_{1 \le i < j \le 4} \left((x_i + x_j)^4 + (x_i - x_j)^4\right) = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2. \quad (4)$$

Many similar and more complicated formulas were found in the late 19th century, until Hilbert showed that they must exist in all degrees.

As one indication of their geometric and combinatorial significance, if you take the the coordinates of the coefficients of the $2\binom{4}{2}$ linear forms in this identity, together with their antipodes, you get the 24 points $(\pm 1, \pm 1, 0, 0)$ and their permutations.

These are the vertices of a regular polytope in $\mathbb{R}^4$ called the *24-cell*.

One idea used a lot in this talk is, I hope, fairly familiar. Suppose $2 \le d \in \mathbb{N}$. Let

$$\zeta_d = e^{\frac{2\pi i}{d}} = \cos\left(\frac{2\pi}{d}\right) + i \sin\left(\frac{2\pi}{d}\right)$$

denote a primitive d-th root of unity: the solutions to the equation $z^d = 1$ are given by $\{\ \zeta_d^k\ :\ 0 \le k \le d-1\}$.

One idea used a lot in this talk is, I hope, fairly familiar. Suppose $2 \le d \in \mathbb{N}$. Let

$$\zeta_d = e^{\frac{2\pi i}{d}} = \cos\left(\frac{2\pi}{d}\right) + i \sin\left(\frac{2\pi}{d}\right)$$

denote a primitive d-th root of unity: the solutions to the equation $z^d = 1$ are given by $\{\ \zeta_d^k\ :\ 0 \le k \le d-1\}$.
Since the sum below is a finite geometric progression, it is easy to see that

Lemma

$$\sum_{r=0}^{d-1} \left(\zeta_d^k\right)^r = \begin{cases} d, & \textit{if } d \mid k; \\ 0, & \textit{otherwise.} \end{cases}$$

We'll use this lemma in sums of polynomials "synched" with powers of ζ_d, so that only every d-th monomial can possibly occur.

Let's look at the first identity again and pull out a factor of 2^{10}:

$$1024x^{10} + 1024y^{10} + (x + \sqrt{3}\, y)^{10} + (x - \sqrt{3}\, y)^{10}$$
$$+(\sqrt{3}\, x + y)^{10} + (\sqrt{3}\, x - y)^{10} = 1512(x^2 + y^2)^5.$$

Let's look at the first identity again and pull out a factor of 2^{10}:

$$1024x^{10} + 1024y^{10} + (x + \sqrt{3}\ y)^{10} + (x - \sqrt{3}\ y)^{10}$$
$$+(\sqrt{3}\ x + y)^{10} + (\sqrt{3}\ x - y)^{10} = 1512(x^2 + y^2)^5.$$

becomes

$$x^{10} + y^{10} + \left(\frac{1}{2}\ x + \frac{\sqrt{3}}{2}\ y\right)^{10} + \left(\frac{1}{2}\ x - \frac{\sqrt{3}}{2}\ y\right)^{10}$$
$$+\left(\frac{\sqrt{3}}{2}\ x + \frac{1}{2}\ y\right)^{10} + \left(\frac{\sqrt{3}}{2}\ x - \frac{1}{2}\ y\right)^{10} = \frac{189}{128}\left(x^2 + y^2\right)^5.$$

Let's look at the first identity again and pull out a factor of 2^{10}:

$$1024x^{10} + 1024y^{10} + (x + \sqrt{3}\ y)^{10} + (x - \sqrt{3}\ y)^{10}$$
$$+(\sqrt{3}\ x + y)^{10} + (\sqrt{3}\ x - y)^{10} = 1512(x^2 + y^2)^5.$$

becomes

$$x^{10} + y^{10} + \left(\frac{1}{2}\ x + \frac{\sqrt{3}}{2}\ y\right)^{10} + \left(\frac{1}{2}\ x - \frac{\sqrt{3}}{2}\ y\right)^{10}$$
$$+\left(\frac{\sqrt{3}}{2}\ x + \frac{1}{2}\ y\right)^{10} + \left(\frac{\sqrt{3}}{2}\ x - \frac{1}{2}\ y\right)^{10} = \frac{189}{128}\left(x^2 + y^2\right)^5.$$

It's looking better already. You may recognize this as

$$\sum_{j=0}^{5} \left(\cos\left(\frac{j\pi}{6}\right) x + \sin\left(\frac{j\pi}{6}\right) y \right)^{10} = \frac{189}{128}(x^2 + y^2)^5.$$

$$\sum_{j=0}^{5}\left(\cos\left(\frac{j\pi}{6}\right)x+\sin\left(\frac{j\pi}{6}\right)y\right)^{10}=\frac{189}{128}(x^2+y^2)^5.$$

(The first explicit appearance I've found of the underlying general theorem below is in a paper of Avner Friedman (1957).)

Theorem

If $d > r$, then for all θ,

$$\sum_{j=0}^{d-1}\left(\cos\left(\frac{2j\pi}{2d}+\theta\right)x+\sin\left(\frac{2j\pi}{2d}+\theta\right)y\right)^{2r} = \frac{d}{2^{2r}}\binom{2r}{r}(x^2+y^2)^r \tag{5}$$

Taking $d=6, r=5$ and $\theta=0$ in (5) and noting $\frac{6}{2^{10}}\binom{10}{5}=\frac{6\cdot 252}{1024}$ $=\frac{1512}{1024}=\frac{189}{128}$, we get (1).

The fastest proof of the Theorem is to derive it from another formula, which uses synching at its best. Expand the left-hand side below, switch the order of summation and recall that $\zeta_{2d}^{2m} = \zeta_d^m$.

$$\sum_{j=0}^{d-1} (\zeta_{2d}^{j} u + \zeta_{2d}^{-j} v)^{2r}$$

The fastest proof of the Theorem is to derive it from another formula, which uses synching at its best. Expand the left-hand side below, switch the order of summation and recall that $\zeta_{2d}^{2m} = \zeta_d^m$.

$$\sum_{j=0}^{d-1} (\zeta_{2d}^{j} u + \zeta_{2d}^{-j} v)^{2r} = \sum_{k=0}^{2r} \binom{2r}{k} \left(\sum_{j=0}^{d-1} \zeta_{2d}^{j(2r-k)+(-j)k} \right) u^{2r-k} v^{k}$$

The fastest proof of the Theorem is to derive it from another formula, which uses synching at its best. Expand the left-hand side below, switch the order of summation and recall that $\zeta_{2d}^{2m} = \zeta_d^m$.

$$\sum_{j=0}^{d-1} (\zeta_{2d}^{j} u + \zeta_{2d}^{-j} v)^{2r} = \sum_{k=0}^{2r} \binom{2r}{k} \left(\sum_{j=0}^{d-1} \zeta_{2d}^{j(2r-k)+(-j)k} \right) u^{2r-k} v^{k}$$

$$= \sum_{k=0}^{2r} \binom{2r}{k} \left(\sum_{j=0}^{d-1} \left(\zeta_{d}^{r-k} \right)^{j} \right) u^{2r-k} v^{k}$$

The fastest proof of the Theorem is to derive it from another formula, which uses synching at its best. Expand the left-hand side below, switch the order of summation and recall that $\zeta_{2d}^{2m} = \zeta_d^m$.

$$\sum_{j=0}^{d-1} (\zeta_{2d}^{j} u + \zeta_{2d}^{-j} v)^{2r} = \sum_{k=0}^{2r} \binom{2r}{k} \left(\sum_{j=0}^{d-1} \zeta_{2d}^{j(2r-k)+(-j)k} \right) u^{2r-k} v^k$$

$$= \sum_{k=0}^{2r} \binom{2r}{k} \left(\sum_{j=0}^{d-1} \left(\zeta_d^{r-k} \right)^j \right) u^{2r-k} v^k$$

As we've seen, the inner sum is zero unless $d \mid r - k$. Since $d > r$, the only multiple of d in $\{-r, -(r-1), \ldots, 0, \ldots, r-1, r\}$ is 0, corresponding to $k = r$, so

$$\sum_{j=0}^{d-1} (\zeta_{2d}^{j} u + \zeta_{2d}^{-j} v)^{2r} = d \binom{2r}{r} u^r v^r.$$

Finally, we substitute $u = \frac{1}{2}e^{i\theta}(x + \frac{y}{i})$ and $v = \frac{1}{2}e^{-i\theta}(x - \frac{y}{i})$ into

$$\sum_{j=0}^{d-1} (\zeta_{2d}^{j} u + \zeta_{2d}^{-j} v)^{2r} = d\binom{2r}{r} u^r v^r.$$

Finally, we substitute $u = \frac{1}{2}e^{i\theta}(x + \frac{y}{i})$ and $v = \frac{1}{2}e^{-i\theta}(x - \frac{y}{i})$ into

$$\sum_{j=0}^{d-1} (\zeta_{2d}^{j} u + \zeta_{2d}^{-j} v)^{2r} = d\binom{2r}{r} u^r v^r.$$

Note that $e^{i\theta} = \cos\theta + i\sin\theta$ and θ doesn't have to be real! By the usual methods, a rearrangement gives

Finally, we substitute $u = \frac{1}{2}e^{i\theta}(x + \frac{y}{i})$ and $v = \frac{1}{2}e^{-i\theta}(x - \frac{y}{i})$ into

$$\sum_{j=0}^{d-1}(\zeta_{2d}^{j}u + \zeta_{2d}^{-j}v)^{2r} = d\binom{2r}{r}u^r v^r.$$

Note that $e^{i\theta} = \cos\theta + i\sin\theta$ and θ doesn't have to be real! By the usual methods, a rearrangement gives

$$\zeta_{2d}^{j}u + \zeta_{2d}^{-j}v = \cos\left(\frac{2j\pi}{2d} + \theta\right)x + \sin\left(\frac{2j\pi}{2d} + \theta\right)y,$$
$$u\ v = \frac{x^2 + y^2}{4},$$

Finally, we substitute $u = \frac{1}{2}e^{i\theta}(x + \frac{y}{i})$ and $v = \frac{1}{2}e^{-i\theta}(x - \frac{y}{i})$ into

$$\sum_{j=0}^{d-1} (\zeta_{2d}^{j} u + \zeta_{2d}^{-j} v)^{2r} = d\binom{2r}{r} u^r v^r.$$

Note that $e^{i\theta} = \cos\theta + i\sin\theta$ and θ doesn't have to be real! By the usual methods, a rearrangement gives

$$\zeta_{2d}^{j} u + \zeta_{2d}^{-j} v = \cos\left(\frac{2j\pi}{2d} + \theta\right) x + \sin\left(\frac{2j\pi}{2d} + \theta\right) y,$$
$$u\ v = \frac{x^2 + y^2}{4},$$

and this proves the Theorem.

Every 19th century math major knew that $\tan(\frac{\pi}{8}) = \sqrt{2} - 1$, so if we take $r = 7$ and $d = 8$ in the Theorem and let $\lambda = 338 + 239\sqrt{2}$ and $\alpha = \sqrt{2} - 1$, and do some minor bookkeeping, we get

Every 19th century math major knew that $\tan(\frac{\pi}{8}) = \sqrt{2} - 1$, so if we take $r = 7$ and $d = 8$ in the Theorem and let $\lambda = 338 + 239\sqrt{2}$ and $\alpha = \sqrt{2} - 1$, and do some minor bookkeeping, we get

$$2048x^{14} + 2048y^{14} + 16(x+y)^{14} + 16(x-y)^{14} +$$
$$\lambda \left((x+\alpha y)^{14} + (x-\alpha y)^{14} + (\alpha x + y)^{14} + (\alpha x - y)^{14} \right)$$
$$= 3432(x^2+y^2)^7.$$

Every 19th century math major knew that $\tan(\frac{\pi}{8}) = \sqrt{2} - 1$, so if we take $r = 7$ and $d = 8$ in (5) and let $\lambda = 338 + 239\sqrt{2}$ and $\alpha = \sqrt{2} - 1$, and do some minor bookkeeping, we get

$$2048x^{14} + 2048y^{14} + 16(x+y)^{14} + 16(x-y)^{14} +$$
$$\lambda\left((x+\alpha y)^{14} + (x-\alpha y)^{14} + (\alpha x + y)^{14} + (\alpha x - y)^{14}\right)$$
$$= 3432(x^2+y^2)^7.$$

To be sure, if you replace $\{\alpha, \lambda, 2048, 16\}$ with unknowns and ask Mathematica to solve for them, it will do so, almost instantaneously.

Every 19th century math major knew that $\tan(\frac{\pi}{8}) = \sqrt{2} - 1$, so if we take $r = 7$ and $d = 8$ in (5) and let $\lambda = 338 + 239\sqrt{2}$ and $\alpha = \sqrt{2} - 1$, and do some minor bookkeeping, we get

$$2048x^{14} + 2048y^{14} + 16(x+y)^{14} + 16(x-y)^{14} + \lambda\left((x+\alpha y)^{14} + (x-\alpha y)^{14} + (\alpha x + y)^{14} + (\alpha x - y)^{14}\right) = 3432(x^2+y^2)^7.$$

To be sure, if you replace $\{\alpha, \lambda, 2048, 16\}$ with unknowns and ask Mathematica to solve for them, it will do so, almost instantaneously.

But it won't know *why*.

Every 19th century math major knew that $\tan(\frac{\pi}{8}) = \sqrt{2} - 1$, so if we take $r = 7$ and $d = 8$ in (5) and let $\lambda = 338 + 239\sqrt{2}$ and $\alpha = \sqrt{2} - 1$, and do some minor bookkeeping, we get

$$2048x^{14} + 2048y^{14} + 16(x+y)^{14} + 16(x-y)^{14} + \\ \lambda\left((x+\alpha y)^{14} + (x-\alpha y)^{14} + (\alpha x + y)^{14} + (\alpha x - y)^{14}\right) \\ = 3432(x^2+y^2)^7.$$

To be sure, if you replace $\{\alpha, \lambda, 2048, 16\}$ with unknowns and ask Mathematica to solve for them, it will do so, almost instantaneously.

But it won't know *why*.

Or appreciate just how astonishingly groovy this identity is!

Every 19th century math major knew that $\tan(\frac{\pi}{8}) = \sqrt{2} - 1$, so if we take $r = 7$ and $d = 8$ in (5) and let $\lambda = 338 + 239\sqrt{2}$ and $\alpha = \sqrt{2} - 1$, and do some minor bookkeeping, we get

$$2048x^{14} + 2048y^{14} + 16(x+y)^{14} + 16(x-y)^{14} +$$
$$\lambda\left((x+\alpha y)^{14} + (x-\alpha y)^{14} + (\alpha x + y)^{14} + (\alpha x - y)^{14}\right)$$
$$= 3432(x^2+y^2)^7.$$

To be sure, if you replace $\{\alpha, \lambda, 2048, 16\}$ with unknowns and ask Mathematica to solve for them, it will do so, almost instantaneously.

But it won't know *why*.

Or appreciate just how astonishingly groovy this identity is!

But it's actually useful, in a formulation that goes back to the 1860's.

Corollary

If $d > r$, $\theta \in \mathbb{R}$ is arbitrary and $p(x, y)$ is a polynomial with degree $\leq 2r + 1$, then

$$\frac{1}{2\pi}\int_0^{2\pi} p(\cos t, \sin t)\ dt$$
$$= \frac{1}{2d}\sum_{j=0}^{2d-1} p\left(\cos\left(\tfrac{2j\pi}{2d} + \theta\right), \sin\left(\tfrac{2j\pi}{2d} + \theta\right)\right).$$

There are similar formulas in > 2 variables, as we'll see later. The main reason these are less explicit than for two variables is this: 2011 points placed evenly on a circle clearly should be the vertices of a regular 2011-gon. How should you place 2011 points "evenly" on the surface of S^{n-1}?

In 1591 (or 1593), François Viète published a revolutionary work on algebra which has been translated into English as *The Analytic Art* by T. R. Witmer. Viète's "Zetetic XVIII" is

> *Given two cubes, to find numerically two other cubes the sum of which is equal to the difference between those that are given.*

In 1591 (or 1593), François Viète published a revolutionary work on algebra which has been translated into English as *The Analytic Art* by T. R. Witmer. Viète's "Zetetic XVIII" is

> *Given two cubes, to find numerically two other cubes the sum of which is equal to the difference between those that are given.*

In 1591 (or 1593), François Viète published a revolutionary work on algebra which has been translated into English as *The Analytic Art* by T. R. Witmer. Viète's "Zetetic XVIII" is

> *Given two cubes, to find numerically two other cubes the sum of which is equal to the difference between those that are given.*

I'll quote Viète's proof on the next page. Keep in mind that he was working at the dawn of algebra, when mathematicians were not yet comfortable with negative numbers and the algebraic conventions were very fluid. Viète used vowels as variables and consonants as constants.

"Let the two given cubes be B^3 and D^3, the first to be greater and the second to be smaller. Two other cubes are to be found, the sum of which is equal to $B^3 - D^3$. Let $B - A$ be the root of the first one that is to be found, and let $B^2A/D^2 - D$ be the root of the second. Forming the cubes and comparing them with $B^3 - D^3$, it will be found that $3D^3B/(B^3 + D^3)$ equals A. The root of the first cube to be found, therefore, is $[B(B^3 - 2D^3)]/(B^3 + D^3)$ and of the second is $[D(2B^3 - D^3)]/(B^3 + D^3)$. And the sum of the two cubes of these is equal to $B^3 - D^3$."

"Let the two given cubes be B^3 and D^3, the first to be greater and the second to be smaller. Two other cubes are to be found, the sum of which is equal to $B^3 - D^3$. Let $B - A$ be the root of the first one that is to be found, and let $B^2A/D^2 - D$ be the root of the second. Forming the cubes and comparing them with $B^3 - D^3$, it will be found that $3D^3B/(B^3 + D^3)$ equals A. The root of the first cube to be found, therefore, is $[B(B^3 - 2D^3)]/(B^3 + D^3)$ and of the second is $[D(2B^3 - D^3)]/(B^3 + D^3)$. And the sum of the two cubes of these is equal to $B^3 - D^3$."

That is,

$$B^3 - D^3 = \left(\frac{B(B^3 - 2D^3)}{B^3 + D^3}\right)^3 + \left(\frac{D(2B^3 - D^3)}{B^3 + D^3}\right)^3.$$

By setting $B = x$ and $D = -y$, Viète's formula becomes (2):

$$x^3 + y^3 = \left(\frac{x(x^3+2y^3)}{x^3-y^3}\right)^3 + \left(\frac{y(y^3+2x^3)}{y^3-x^3}\right)^3.$$

We'll explain later just how smart Viète was to choose the coefficients he used.

By setting $B = x$ and $D = -y$, Viète's formula becomes (2):

$$x^3 + y^3 = \left(\frac{x(x^3 + 2y^3)}{x^3 - y^3}\right)^3 + \left(\frac{y(y^3 + 2x^3)}{y^3 - x^3}\right)^3.$$

We'll explain later just how smart Viète was to choose the coefficients he used.
Former UIUC postdoc Jeremy Rouse and I have just written a paper in which we examine the more general equation

$$x^3 + y^3 = p^3(x,y) + q^3(x,y) \tag{6}$$

for homogeneous rational functions $p, q \in \mathbb{C}(x,y)$. You can find it on the arXiv, and it will appear in the IJNT.

To examine this equation, we take a common denominator for the rational functions p, q and rewrite as:

$$x^3 + y^3 = \left(\frac{f(x,y)}{h(x,y)}\right)^3 + \left(\frac{g(x,y)}{h(x,y)}\right)^3$$

To examine this equation, we take a common denominator for the rational functions p, q and rewrite as:

$$\begin{aligned} x^3 + y^3 &= \left(\frac{f(x,y)}{h(x,y)}\right)^3 + \left(\frac{g(x,y)}{h(x,y)}\right)^3 \\ \implies h(x,y)^3(x^3+y^3) &= f(x,y)^3 + g(x,y)^3. \end{aligned} \tag{7}$$

To examine this equation, we take a common denominator for the rational functions p, q and rewrite as:

$$
\begin{aligned}
x^3 + y^3 &= \left(\frac{f(x,y)}{h(x,y)}\right)^3 + \left(\frac{g(x,y)}{h(x,y)}\right)^3 \\
\implies h(x,y)^3(x^3+y^3) &= f(x,y)^3 + g(x,y)^3.
\end{aligned}
\tag{7}
$$

It follows that if $\pi(x,y)$ is irreducible and π divides any two of $\{f, g, h\}$, then it divides the third. Also note that f and g may be permuted and cube roots of unity ω^j may appear. Assume that f, g, h are forms (that is, homogeneous). If $\deg f = \deg g = d$, then we call (7) a *solution of degree d*.

Here is a roster of all the solutions of degree ≤ 11.

There's an obvious solution of degree 1: $(f, g, h) = (x, y, 1)$.
Viète's solution has degree 4, but there's also one of degree 3.

Here is a roster of all the solutions of degree ≤ 11.

There's an obvious solution of degree 1: $(f, g, h) = (x, y, 1)$. Viète's solution has degree 4, but there's also one of degree 3. Let $\zeta = \zeta_{12} = \frac{\sqrt{3}}{2} + \frac{i}{2}$, and observe that $\zeta + \zeta^{-1} = \sqrt{3}$ and $\zeta^3 + \zeta^{-3} = i - i = 0$.

Here is a roster of all the solutions of degree ≤ 11.

There's an obvious solution of degree 1: $(f, g, h) = (x, y, 1)$.
Viète's solution has degree 4, but there's also one of degree 3.
Let $\zeta = \zeta_{12} = \frac{\sqrt{3}}{2} + \frac{i}{2}$, and observe that $\zeta + \zeta^{-1} = \sqrt{3}$ and $\zeta^3 + \zeta^{-3} = i - i = 0$. Then

$$(\zeta u + \zeta^{-1} v)^3 + (\zeta^{-1} u + \zeta v)^3$$
$$= (\zeta^3 + \zeta^{-3})(u^3 + v^3) + 3(\zeta + \zeta^{-1})(u^2 v + u v^2)$$

Here is a roster of all the solutions of degree ≤ 11.

There's an obvious solution of degree 1: $(f, g, h) = (x, y, 1)$. Viète's solution has degree 4, but there's also one of degree 3. Let $\zeta = \zeta_{12} = \frac{\sqrt{3}}{2} + \frac{i}{2}$, and observe that $\zeta + \zeta^{-1} = \sqrt{3}$ and $\zeta^3 + \zeta^{-3} = i - i = 0$. Then

$$
\begin{aligned}
&(\zeta u + \zeta^{-1} v)^3 + (\zeta^{-1} u + \zeta v)^3 \\
&= (\zeta^3 + \zeta^{-3})(u^3 + v^3) + 3(\zeta + \zeta^{-1})(u^2 v + uv^2) \\
&= 3\sqrt{3} uv(u + v).
\end{aligned}
$$

Here is a roster of all the solutions of degree ≤ 11.

There's an obvious solution of degree 1: $(f, g, h) = (x, y, 1)$. Viète's solution has degree 4, but there's also one of degree 3. Let $\zeta = \zeta_{12} = \frac{\sqrt{3}}{2} + \frac{i}{2}$, and observe that $\zeta + \zeta^{-1} = \sqrt{3}$ and $\zeta^3 + \zeta^{-3} = i - i = 0$. Then

$$\begin{aligned}
&(\zeta u + \zeta^{-1} v)^3 + (\zeta^{-1} u + \zeta v)^3 \\
&= (\zeta^3 + \zeta^{-3})(u^3 + v^3) + 3(\zeta + \zeta^{-1})(u^2 v + u v^2) \\
&= 3\sqrt{3} uv(u + v).
\end{aligned}$$

After $(u, v) \mapsto (x^3, y^3)$, this rearranges to:

$$x^3 + y^3 = \left(\frac{\zeta x^3 + \zeta^{-1} y^3}{\sqrt{3} xy}\right)^3 + \left(\frac{\zeta^{-1} x^3 + \zeta y^3}{\sqrt{3} xy}\right)^3. \qquad (8)$$

Here is a roster of all the solutions of degree ≤ 11.

There's an obvious solution of degree 1: $(f, g, h) = (x, y, 1)$.
Viète's solution has degree 4, but there's also one of degree 3.
Let $\zeta = \zeta_{12} = \frac{\sqrt{3}}{2} + \frac{i}{2}$, and observe that $\zeta + \zeta^{-1} = \sqrt{3}$ and $\zeta^3 + \zeta^{-3} = i - i = 0$. Then

$$\begin{aligned}(\zeta u + \zeta^{-1} v)^3 + (\zeta^{-1} u + \zeta v)^3 \\ = (\zeta^3 + \zeta^{-3})(u^3 + v^3) + 3(\zeta + \zeta^{-1})(u^2 v + u v^2) \\ = 3\sqrt{3} uv(u + v).\end{aligned}$$

After $(u, v) \mapsto (x^3, y^3)$, this rearranges to:

$$x^3 + y^3 = \left(\frac{\zeta x^3 + \zeta^{-1} y^3}{\sqrt{3} xy}\right)^3 + \left(\frac{\zeta^{-1} x^3 + \zeta y^3}{\sqrt{3} xy}\right)^3. \qquad (8)$$

Let's call this the *small* solution.

There are two solutions of degree 7 which are complex conjugates of each other. Here's one of them.

$$f(x,y) = x(x^6 + (-1 + 3\sqrt{3}i)(x^3y^3 + y^6)),$$
$$g(x,y) = y((-1 + 3\sqrt{3}i)(x^6 + x^3y^3) + y^6),$$
$$h(x,y) = x^6 + \left(\frac{5 - 3\sqrt{3}i}{2}\right)x^3y^3 + y^6.$$

There are two solutions of degree 7 which are complex conjugates of each other. Here's one of them.

$$f(x,y) = x(x^6 + (-1+3\sqrt{3}i)(x^3y^3 + y^6)),$$
$$g(x,y) = y((-1+3\sqrt{3}i)(x^6 + x^3y^3) + y^6),$$
$$h(x,y) = x^6 + \left(\frac{5-3\sqrt{3}i}{2}\right)x^3y^3 + y^6.$$

There is one degree 9 solution, with real integral coefficients:

$$f(x,y) = x^9 + 6x^6y^3 + 3x^3y^6 - y^9,$$
$$g(x,y) = -x^9 + 3x^6y^3 + 6x^3y^6 + y^9,$$
$$h(x,y) = 3xy(x^6 + x^3y^3 + y^6).$$

In addition to the symmetries mentioned earlier, there is a natural composition of two solutions to the Viéte equation. Suppose

$$x^3 + y^3 = p_1^3(x,y) + q_1^3(x,y) = p_2^3(x,y) + q_2^3(x,y).$$

Then if we compose the solutions, we see that

$$p_1^3(p_2(x,y), q_2(x,y)) + q_1^3(p_2(x,y), q_2(x,y)) \\ = p_2^3(x,y) + q_2^3(x,y) = x^3 + y^3.$$

Accordingly, we define $(p_1, q_1) \circ (p_2, q_2) = (p_3, q_3)$ by

$$p_3(x,y) = p_1(p_2(x,y), q_2(x,y)); q_3(x,y) = q_1(p_2(x,y), q_2(x,y)).$$

In addition to the symmetries mentioned earlier, there is a natural composition of two solutions to the Viéte equation. Suppose

$$x^3 + y^3 = p_1^3(x,y) + q_1^3(x,y) = p_2^3(x,y) + q_2^3(x,y).$$

Then if we compose the solutions, we see that

$$p_1^3(p_2(x,y), q_2(x,y)) + q_1^3(p_2(x,y), q_2(x,y)) \\ = p_2^3(x,y) + q_2^3(x,y) = x^3 + y^3.$$

Accordingly, we define $(p_1, q_1) \circ (p_2, q_2) = (p_3, q_3)$ by

$$p_3(x,y) = p_1(p_2(x,y), q_2(x,y)); q_3(x,y) = q_1(p_2(x,y), q_2(x,y)).$$

The small solution composed with itself gives the (real) degree 9 solution: the roots of unity cancel!
Viète's solution and the small solution commute, giving the (unique) solution of degree 12, which is not written here.

As part of an explanation, we use a theorem which might well have been known in the 19th century literature.

Theorem

Suppose $p \in \mathbb{C}[x_1, \dots, x_n]$*. Then there exist* $f, g \in \mathbb{C}[x_1, \dots, x_n]$ *such that* $p = f^3 + g^3$ *if and only if* p *is a cube, or* $p = q_1 q_2 q_3$*, where* q_i*'s are linearly dependent, but pairwise non-proportional.*

As part of an explanation, we use a theorem which might well have been known in the 19th century literature.

Theorem

Suppose $p \in \mathbb{C}[x_1, \ldots, x_n]$. *Then there exist* $f, g \in \mathbb{C}[x_1, \ldots, x_n]$ *such that* $p = f^3 + g^3$ *if and only if* p *is a cube, or* $p = q_1 q_2 q_3$, *where* q_i*'s are linearly dependent, but pairwise non-proportional.*

Proof.

Assume p is not a cube. Then $p = (f+g)(f+\omega g)(f+\omega^2 g)$ is such a factorization.

As part of an explanation, we use a theorem which might well have been known in the 19th century literature.

Theorem

Suppose $p \in \mathbb{C}[x_1, \dots, x_n]$. Then there exist $f, g \in \mathbb{C}[x_1, \dots, x_n]$ such that $p = f^3 + g^3$ if and only if p is a cube, or $p = q_1 q_2 q_3$, where q_i's are linearly dependent, but pairwise non-proportional.

Proof.

Assume p is not a cube. Then $p = (f + g)(f + \omega g)(f + \omega^2 g)$ is such a factorization.

As part of an explanation, we use a theorem which might well have been known in the 19th century literature.

Theorem

Suppose $p \in \mathbb{C}[x_1, \ldots, x_n]$. Then there exist $f, g \in \mathbb{C}[x_1, \ldots, x_n]$ such that $p = f^3 + g^3$ if and only if p is a cube, or $p = q_1 q_2 q_3$, where q_i's are linearly dependent, but pairwise non-proportional.

Proof.

Assume p is not a cube. Then $p = (f+g)(f+\omega g)(f+\omega^2 g)$ is such a factorization.
Conversely, if $p = q_1 q_2 q_3$ and $q_3 = a q_1 + b q_2$ with $ab \neq 0$, then

$$\left(\frac{\zeta\ a\ q_1 + \zeta^{-1}\ b\ q_2}{\sqrt{3}(ab)^{1/3}}\right)^3 + \left(\frac{\zeta^{-1}\ a\ q_1 + \zeta\ b\ q_2}{\sqrt{3}(ab)^{1/3}}\right)^3$$
$$= q_1 q_2 (a\ q_1 + b\ q_2) = p.$$

This is essentially the small solution again. □

This theorem can used to analyze $(x^3 + y^3)h(x, y)^3$. For example, $\{x^3, y^3, (x^3 + y^3)\}$ is linearly dependent, hence $x^3y^3(x^3 + y^3)$ is a sum of two cubes. This leads to the small solution.

This theorem can used to analyze $(x^3 + y^3)h(x, y)^3$. For example, $\{x^3, y^3, (x^3 + y^3)\}$ is linearly dependent, hence $x^3y^3(x^3 + y^3)$ is a sum of two cubes. This leads to the small solution.
Less trivially, looking at the exponents mod 3, we see that

$$(x + y)(x - y)^3 = (x^4 + 2xy^3) - (2x^3y + y^4)$$
$$(x + \omega y)(x - \omega y)^3 = (x^4 + 2xy^3) - \omega(2x^3y + y^4)$$
$$(x + \omega^2 y)(x - \omega^2 y)^3 = (x^4 + 2xy^3) - \omega^2(2x^3y + y^4)$$

This theorem can used to analyze $(x^3+y^3)h(x,y)^3$. For example, $\{x^3, y^3, (x^3+y^3)\}$ is linearly dependent, hence $x^3y^3(x^3+y^3)$ is a sum of two cubes. This leads to the small solution.
Less trivially, looking at the exponents mod 3, we see that

$$(x+y)(x-y)^3 = (x^4+2xy^3) - (2x^3y+y^4)$$
$$(x+\omega y)(x-\omega y)^3 = (x^4+2xy^3) - \omega(2x^3y+y^4)$$
$$(x+\omega^2 y)(x-\omega^2 y)^3 = (x^4+2xy^3) - \omega^2(2x^3y+y^4)$$

are linearly dependent, hence their product,

$$(x+y)(x+\omega y)(x+\omega^2 y)(x-y)^3(x-\omega y)^3(x-\omega^2 y)^3$$
$$= (x^3+y^3)(x^3-y^3)^3,$$

is a sum of two cubes. If you work out the details, you recover Viéte's (2).

Elliptic curve people know that the line through two points on the curve $X^3 + Y^3 = A$ intersects the curve in a third point, which, after reflection, is called the *sum* of the two points. This defines an abelian group.

Elliptic curve people know that the line through two points on the curve $X^3 + Y^3 = A$ intersects the curve in a third point, which, after reflection, is called the *sum* of the two points. This defines an abelian group.

Assuming $X_j^3 + Y_j^3 = A$, the addition law works out to be

$$(X_1, Y_1) + (X_2, Y_2) = (X_3, Y_3),$$

where

$$X_3 = \frac{A(Y_1 - Y_2) + X_1X_2(X_1Y_2 - X_2Y_1)}{(X_1^2X_2 + Y_1^2Y_2) - (X_1X_2^2 + Y_1Y_2^2)},$$

$$Y_3 = \frac{A(X_1 - X_2) + Y_1Y_2(X_2Y_1 - X_1Y_2)}{(X_1^2X_2 + Y_1^2Y_2) - (X_1X_2^2 + Y_1Y_2^2)}.$$

But this formula breaks down when the two points coincide; instead, take a line tangent to the curve at (X_1, Y_1). By implicit differentiation, the slope is $-\frac{X_1^2}{Y_1^2}$ and we seek t so that

$$(X_1 - t)^3 + \left(Y_1 + t \cdot \frac{X_1^2}{Y_1^2}\right)^3 = X_1^3 + Y_1^3$$

It turns out that there is a double root at $t = 0$ and a single root at $t = -\frac{3X_1 Y_1^3}{X_1^3 - Y_1^3}$. Putting this value of t above gives Viète's identity.

But this formula breaks down when the two points coincide; instead, take a line tangent to the curve at (X_1, Y_1). By implicit differentiation, the slope is $-\frac{X_1^2}{Y_1^2}$ and we seek t so that

$$(X_1 - t)^3 + \left(Y_1 + t \cdot \frac{X_1^2}{Y_1^2}\right)^3 = X_1^3 + Y_1^3$$

It turns out that there is a double root at $t = 0$ and a single root at $t = -\frac{3X_1Y_1^3}{X_1^3 - Y_1^3}$. Putting this value of t above gives Viète's identity. Believe it or not, this is, formally, what Viète was doing! I doubt he knew about elliptic curves (he was working before Cartesian coordinates had been invented), but he was one of the first people to study cubics. He must have known that his particular substitution would give a double root at zero, leaving the third root rational.

Let's suppose $X, Y, A \in \mathbb{C}(t)$, and $A = 1 + t^3$. Then our equation is

$$X^3(t) + Y^3(t) = 1 + t^3 \tag{9}$$

and if we homogenize (9), by setting $t = y/x$ and multiplying both sides by x^3, then we get (6). In order to fit in this interpretation, though, keep in mind that every solution (p, q) corresponds to 18 points on the curve (9): $(\omega^j p, \omega^k q)$ and $(\omega^j q, \omega^k p)$, $0 \le j, k \le 2$.

Let's suppose $X, Y, A \in \mathbb{C}(t)$, and $A = 1 + t^3$. Then our equation is

$$X^3(t) + Y^3(t) = 1 + t^3 \tag{9}$$

and if we homogenize (9), by setting $t = y/x$ and multiplying both sides by x^3, then we get (6). In order to fit in this interpretation, though, keep in mind that every solution (p, q) corresponds to 18 points on the curve (9): $(\omega^j p, \omega^k q)$ and $(\omega^j q, \omega^k p)$, $0 \le j, k \le 2$.

The famous Mordell-Weil Theorem says that the group of rational points on an elliptic curve is finitely generated, and it also applies to curves over $\mathbb{C}(t)$ such as this. Under the definition given above, Viète's solution turns out to be $-2(x, y)$ and the small solution is $(x, y) + 2(\omega x, \omega y)$.

We recall notation and give our joint results with Rouse. Suppose

$$x^3 + y^3 = p^3(x,y) + q^3(x,y) = \left(\frac{f(x,y)}{h(x,y)}\right)^3 + \left(\frac{g(x,y)}{h(x,y)}\right)^3$$

and the solution has degree d. Then:

We recall notation and give our joint results with Rouse. Suppose

$$x^3 + y^3 = p^3(x,y) + q^3(x,y) = \left(\frac{f(x,y)}{h(x,y)}\right)^3 + \left(\frac{g(x,y)}{h(x,y)}\right)^3$$

and the solution has degree d. Then:

- $q(x,y) = p(y,x)$ (up to powers of ω).

We recall notation and give our joint results with Rouse. Suppose

$$x^3 + y^3 = p^3(x,y) + q^3(x,y) = \left(\frac{f(x,y)}{h(x,y)}\right)^3 + \left(\frac{g(x,y)}{h(x,y)}\right)^3$$

and the solution has degree d. Then:

- $q(x,y) = p(y,x)$ (up to powers of ω).
- $p, q \in \mathbb{Q}(\omega)(x,y)$.

We recall notation and give our joint results with Rouse. Suppose

$$x^3 + y^3 = p^3(x,y) + q^3(x,y) = \left(\frac{f(x,y)}{h(x,y)}\right)^3 + \left(\frac{g(x,y)}{h(x,y)}\right)^3$$

and the solution has degree d. Then:

- $q(x,y) = p(y,x)$ (up to powers of ω).
- $p, q \in \mathbb{Q}(\omega)(x,y)$.
- There is a solution in $\mathbb{Q}(x,y)$ iff d is a square (e.g., $d = 4, 9$.)

We recall notation and give our joint results with Rouse. Suppose

$$x^3 + y^3 = p^3(x,y) + q^3(x,y) = \left(\frac{f(x,y)}{h(x,y)}\right)^3 + \left(\frac{g(x,y)}{h(x,y)}\right)^3$$

and the solution has degree d. Then:

- $q(x,y) = p(y,x)$ (up to powers of ω).
- $p, q \in \mathbb{Q}(\omega)(x,y)$.
- There is a solution in $\mathbb{Q}(x,y)$ iff d is a square (e.g., $d = 4, 9$.)
- Any two solutions commute under composition, up to multiplication by cube roots of unity.

We recall notation and give our joint results with Rouse. Suppose

$$x^3 + y^3 = p^3(x,y) + q^3(x,y) = \left(\frac{f(x,y)}{h(x,y)}\right)^3 + \left(\frac{g(x,y)}{h(x,y)}\right)^3$$

and the solution has degree d. Then:

- $q(x,y) = p(y,x)$ (up to powers of ω).
- $p, q \in \mathbb{Q}(\omega)(x,y)$.
- There is a solution in $\mathbb{Q}(x,y)$ iff d is a square (e.g., $d = 4, 9$.)
- Any two solutions commute under composition, up to multiplication by cube roots of unity.
- Any solution of degree $3k$ is the composition of the small solution with a solution of degree k.

We recall notation and give our joint results with Rouse. Suppose

$$x^3 + y^3 = p^3(x,y) + q^3(x,y) = \left(\frac{f(x,y)}{h(x,y)}\right)^3 + \left(\frac{g(x,y)}{h(x,y)}\right)^3$$

and the solution has degree d. Then:

- $q(x,y) = p(y,x)$ (up to powers of ω).
- $p, q \in \mathbb{Q}(\omega)(x,y)$.
- There is a solution in $\mathbb{Q}(x,y)$ iff d is a square (e.g., $d = 4, 9$.)
- Any two solutions commute under composition, up to multiplication by cube roots of unity.
- Any solution of degree $3k$ is the composition of the small solution with a solution of degree k.
- No monomial occuring in any f, g, h has an exponent $\equiv 2 \bmod 3$.

- The set of solutions form the group $\mathbb{Z} + \mathbb{Z} + \mathbb{Z}_3$, with generators (x, y), $(\omega x, \omega y)$ and torsion involving ω^j. The solution $m(x, y) + n(\omega x, \omega y)$ has degree $m^2 - mn + n^2$.

- The set of solutions form the group $\mathbb{Z}+\mathbb{Z}+\mathbb{Z}_3$, with generators (x,y), $(\omega x,\omega y)$ and torsion involving ω^j. The solution $m(x,y)+n(\omega x,\omega y)$ has degree m^2-mn+n^2.
- The subgroup $\mathbb{Z}+\mathbb{Z}$ is actually **ring**-homomorphic to $\mathbb{Z}[\omega]$, under the operations of addition of points and composition.

- The set of solutions form the group $\mathbb{Z} + \mathbb{Z} + \mathbb{Z}_3$, with generators (x, y), $(\omega x, \omega y)$ and torsion involving ω^j. The solution $m(x, y) + n(\omega x, \omega y)$ has degree $m^2 - mn + n^2$.
- The subgroup $\mathbb{Z} + \mathbb{Z}$ is actually **ring**-homomorphic to $\mathbb{Z}[\omega]$, under the operations of addition of points and composition.
- Let $a(d)$ denote the number of solutions of degree d, then

$$1 + 6\sum_{d=1}^{\infty} a(d)x^d = \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} x^{m^2-mn+n^2} \implies^{(Lorenz, Ramanujan)}$$

$$\sum_{d=1}^{\infty} a(d)z^d = \sum_{i=0}^{\infty} \left(\frac{x^{3i+1}}{1-x^{3i+1}} - \frac{x^{3i+2}}{1-x^{3i+2}} \right).$$

- The set of solutions form the group $\mathbb{Z}+\mathbb{Z}+\mathbb{Z}_3$, with generators (x,y), $(\omega x,\omega y)$ and torsion involving ω^j. The solution $m(x,y)+n(\omega x,\omega y)$ has degree m^2-mn+n^2.
- The subgroup $\mathbb{Z}+\mathbb{Z}$ is actually **ring**-homomorphic to $\mathbb{Z}[\omega]$, under the operations of addition of points and composition.
- Let $a(d)$ denote the number of solutions of degree d, then

$$1+6\sum_{d=1}^{\infty}a(d)x^d=\sum_{m=-\infty}^{\infty}\sum_{n=-\infty}^{\infty}x^{m^2-mn+n^2} \implies (Lorenz, Ramanujan)$$

$$\sum_{d=1}^{\infty}a(d)z^d=\sum_{i=0}^{\infty}\left(\frac{x^{3i+1}}{1-x^{3i+1}}-\frac{x^{3i+2}}{1-x^{3i+2}}\right).$$

- The number of solutions of degree d is the number of factors of d congruent to 1 mod 3 minus the number congruent to 2 mod 3. Any degree has the form $m^2\prod_j p_j$, $p_j\equiv 1 \bmod 3$.

Recall (3), proved by Desboves (1880) and Elkies (1995): let

$$f_1(x,y) = x^2 + \sqrt{2}\ x\ y - y^2, f_2(x,y) = i\ x^2 - \sqrt{2}\ x\ y + i\ y^2$$
$$f_3(x,y) = -x^2 + \sqrt{2}\ x\ y + y^2, f_4(x,y) = -i\ x^2 - \sqrt{2}\ x\ y - i\ y^2$$

Then $\sum_{i=1}^{4} f_i^5 = 0$.

Recall (3), proved by Desboves (1880) and Elkies (1995): let

$$f_1(x,y) = x^2 + \sqrt{2}\ x\ y - y^2, f_2(x,y) = i\ x^2 - \sqrt{2}\ x\ y + i\ y^2$$
$$f_3(x,y) = -x^2 + \sqrt{2}\ x\ y + y^2, f_4(x,y) = -i\ x^2 - \sqrt{2}\ x\ y - i\ y^2$$

Then $\sum_{i=1}^{4} f_i^5 = 0$.
This was derived by taking the sum

$$\sum_{k=0}^{3} (i^k x^2 + i^{2k} a\ x\ y + i^{3k} y^2)^5 = 40a(a^2+2)(x^7y^3 + x^3y^7),$$

and setting first $a = \sqrt{-2}$ and then $y \mapsto iy$.

Recall (3), proved by Desboves (1880) and Elkies (1995): let

$$f_1(x,y) = x^2 + \sqrt{2}\ x\ y - y^2, f_2(x,y) = i\ x^2 - \sqrt{2}\ x\ y + i\ y^2$$
$$f_3(x,y) = -x^2 + \sqrt{2}\ x\ y + y^2, f_4(x,y) = -i\ x^2 - \sqrt{2}\ x\ y - i\ y^2$$

Then $\sum_{i=1}^4 f_i^5 = 0$.

This was derived by taking the sum

$$\sum_{k=0}^{3} (i^k x^2 + i^{2k} a\ x\ y + i^{3k} y^2)^5 = 40a(a^2+2)(x^7y^3 + x^3y^7),$$

and setting first $a = \sqrt{-2}$ and then $y \mapsto iy$.

The interplay of the roots of unity makes it unsurprising that

$$\sum_{i=1}^{4} f_i = \sum_{i=1}^{4} f_i^2 = 0$$

as well. This is actually, however, too much of a good thing.

Note that the equations $\sum f_i = \sum f_i^2 = 0$ define the intersection of a plane and a sphere in $\mathbb{C}^4$. This is, projectively, a curve. Unless something special is going on, this curve shouldn't contain another curve (f_1, f_2, f_3, f_4).

Note that the equations $\sum f_i = \sum f_i^2 = 0$ define the intersection of a plane and a sphere in $\mathbb{C}^4$. This is, projectively, a curve. Unless something special is going on, this curve shouldn't contain another curve (f_1, f_2, f_3, f_4).
What's special is that the ideal generated by $\sum_{i=1}^4 x_i$ and $\sum_{i=1}^4 x_i^2$ contains $\sum_{i=1}^4 x_i^5$. Proof in a bit.

Note that the equations $\sum f_i = \sum f_i^2 = 0$ define the intersection of a plane and a sphere in $\mathbb{C}^4$. This is, projectively, a curve. Unless something special is going on, this curve shouldn't contain another curve (f_1, f_2, f_3, f_4).

What's special is that the ideal generated by $\sum_{i=1}^4 x_i$ and $\sum_{i=1}^4 x_i^2$ contains $\sum_{i=1}^4 x_i^5$. Proof in a bit.

If $f_4 = -(f_1 + f_2 + f_3)$, then the sum of squares becomes essentially a Pythagorean triple, which we know how to parameterize:

$$f_1^2 + f_2^2 + f_3^2 + (f_1 + f_2 + f_3)^2 = 0 \implies$$

Note that the equations $\sum f_i = \sum f_i^2 = 0$ define the intersection of a plane and a sphere in $\mathbb{C}^4$. This is, projectively, a curve. Unless something special is going on, this curve shouldn't contain another curve (f_1, f_2, f_3, f_4).
What's special is that the ideal generated by $\sum_{i=1}^4 x_i$ and $\sum_{i=1}^4 x_i^2$ contains $\sum_{i=1}^4 x_i^5$. Proof in a bit.
If $f_4 = -(f_1 + f_2 + f_3)$, then the sum of squares becomes essentially a Pythagorean triple, which we know how to parameterize:

$$f_1^2 + f_2^2 + f_3^2 + (f_1 + f_2 + f_3)^2 = 0 \implies$$
$$(f_1 - f_3)^2 + 2(f_1 + f_3)^2 = -(f_1 + 2f_2 + f_3)^2 \quad \text{“} \implies \text{”}$$

Note that the equations $\sum f_i = \sum f_i^2 = 0$ define the intersection of a plane and a sphere in $\mathbb{C}^4$. This is, projectively, a curve. Unless something special is going on, this curve shouldn't contain another curve (f_1, f_2, f_3, f_4).

What's special is that the ideal generated by $\sum_{i=1}^4 x_i$ and $\sum_{i=1}^4 x_i^2$ contains $\sum_{i=1}^4 x_i^5$. Proof in a bit.

If $f_4 = -(f_1 + f_2 + f_3)$, then the sum of squares becomes essentially a Pythagorean triple, which we know how to parameterize:

$$f_1^2 + f_2^2 + f_3^2 + (f_1 + f_2 + f_3)^2 = 0 \implies$$

$$(f_1 - f_3)^2 + 2(f_1 + f_3)^2 = -(f_1 + 2f_2 + f_3)^2 \quad \text{“} \implies \text{”}$$

$$f_1 - f_3 = x^2 - y^2, \sqrt{2}(f_1 + f_3) = 2xy, -i(f_1 + 2f_2 + f_3) = x^2 + y^2$$

We can solve for the f_i's to recover the Desboves-Elkies example.

We could also try to synch a solution. Let $\omega = \zeta_3$.

$$f_1 = x^2 + axy + y^2$$
$$f_2 = \omega x^2 + axy + \omega^2 y^2$$
$$f_3 = \omega^2 x^2 + axy + \omega y^2$$
$$\implies f_1 + f_2 + f_3 = 3axy, \quad f_1^2 + f_2^2 + f_3^2 = 3(a^2+2)x^2y^2.$$

Let $f_4 = -3axy$; $3(a^2+2) + (3a)^2 = 6(2a^2+1) = 0$ implies $a = \sqrt{-1/2}$ to give another solution. Again set $y \to iy$, then

$$(x^2 + \sqrt{1/2}\,xy - y^2)^5 + (\omega x^2 + \sqrt{1/2}\,xy - \omega^2 y^2)^5 +$$
$$(\omega^2 x^2 + \sqrt{1/2}\,xy - \omega y^2)^5 + (-3\sqrt{1/2}\,xy)^5 = 0.$$

This is actually the same as the Desboves-Elkies (3) after a change of variables. Felix Klein smiles.

The relationship of $\sum x_1, \sum x_1^2, \sum x_i^5$ has a larger explanation.

Theorem

If $p(x_1, x_2, x_3, x_4)$ is any symmetric form of degree 5, then $p \in I = (\sum_{i=1}^4 x_i, \sum_{i=1}^4 x_i^2)$.

The relationship of $\sum x_1, \sum x_1^2, \sum x_i^5$ has a larger explanation.

Theorem

If $p(x_1, x_2, x_3, x_4)$ is any symmetric form of degree 5, then $p \in I = (\sum_{i=1}^4 x_i, \sum_{i=1}^4 x_i^2)$.

The relationship of $\sum x_1, \sum x_1^2, \sum x_i^5$ has a larger explanation.

Theorem

If $p(x_1, x_2, x_3, x_4)$ is any symmetric form of degree 5, then $p \in I = (\sum_{i=1}^4 x_i, \sum_{i=1}^4 x_i^2)$.

Proof.

Let e_j denote the usual j-th elementary symmetric function. Since $\sum_{i=1}^4 x_i = e_1$ and $\sum_{i=1}^4 x_i^2 = e_1^2 - 2e_1$, $I = (e_1, e_2)$. By Newton's theorem, any symmetric quintic has the form $c_1 e_1^5 + c_2 e_1^3 e_2$ $+ c_3 e_1^2 e_3 + c_4 e_1 e_4 + c_5 e_1 e_2^2 + c_6 e_2 e_3$, and so is in I. □

The relationship of $\sum x_1, \sum x_1^2, \sum x_i^5$ has a larger explanation.

Theorem

If $p(x_1, x_2, x_3, x_4)$ is any symmetric form of degree 5, then $p \in I = (\sum_{i=1}^4 x_i, \sum_{i=1}^4 x_i^2)$.

Proof.

Let e_j denote the usual j-th elementary symmetric function. Since $\sum_{i=1}^4 x_i = e_1$ and $\sum_{i=1}^4 x_i^2 = e_1^2 - 2e_1$, $I = (e_1, e_2)$. By Newton's theorem, any symmetric quintic has the form $c_1 e_1^5 + c_2 e_1^3 e_2$ $+ c_3 e_1^2 e_3 + c_4 e_1 e_4 + c_5 e_1 e_2^2 + c_6 e_2 e_3$, and so is in I. □

The relationship of $\sum x_1, \sum x_1^2, \sum x_i^5$ has a larger explanation.

Theorem

If $p(x_1, x_2, x_3, x_4)$ is any symmetric form of degree 5, then $p \in I = (\sum_{i=1}^4 x_i, \sum_{i=1}^4 x_i^2)$.

Proof.

Let e_j denote the usual j-th elementary symmetric function. Since $\sum_{i=1}^4 x_i = e_1$ and $\sum_{i=1}^4 x_i^2 = e_1^2 - 2e_1$, $I = (e_1, e_2)$. By Newton's theorem, any symmetric quintic has the form $c_1 e_1^5 + c_2 e_1^3 e_2$ $+ c_3 e_1^2 e_3 + c_4 e_1 e_4 + c_5 e_1 e_2^2 + c_6 e_2 e_3$, and so is in I. □

The proof works because 5 cannot be written as a non-negative integer combination of 3 and 4, a case of the Frobenius problem. Let m and n be relatively prime positive integers > 1 and let $A(m, n)$ be the set of positive integers which **cannot** be written as $am + bn$ for non-negative integers (a, b). Sylvester showed in 1884 that $\max A(m, n) = mn - m - n$.

More generally, let $M_{n,k}(x_1,\ldots,x_n) = \sum_{j=1}^n x_j^k$. A similar argument to the foregoing proves the following theorem.

Theorem

Suppose $x \in \mathbb{C}^n$ is such that $M_{n,r}(x) = 0$ for $r = 1,\ldots,n-2$. If $N \in A(n-1,n)$, then $M_{n,N}(x) = 0$ as well. Alternatively, if N is not expressible as $a(n-1)+bn$, then

$$\sum_{j=1}^n x_j^N \in \left(\sum_{j=1}^n x_j, \sum_{j=1}^n x_j^2, \ldots, \sum_{j=1}^n x_j^{n-2} \right).$$

Note that if $n = 4$, then $A(3,4) = \{1,2,5\}$. This completes the derivation of (3). The largest element in $A(n-1,n)$ is n^2-3n+1. For $n \geq 5$, the intersection $\cap_{r=1}^{n-2} M_{n,r}$ has positive genus and so has no polynomial parameterization: despite the Theorem, there are no versions of Desboves-Elkies in higher degrees.

Mathematica and I spent some time searching for other "interesting" synching identities, and found this one:

$$\sum_{k=0}^{4} (\zeta_5^k x^2 + a\ x\ y + \zeta_5^{-k})^{14} =$$
$$f(a)(x^{24}y^4 + x^4y^{24}) + g(a)(x^{19}y^9 + x^9y^{19}) + h(a)x^{14}y^{14}$$

Mathematica and I spent some time searching for other "interesting" synching identities, and found this one:

$$\sum_{k=0}^{4} (\zeta_5^k x^2 + a\ x\ y + \zeta_5^{-k})^{14} =$$

$$f(a)(x^{24}y^4 + x^4y^{24}) + g(a)(x^{19}y^9 + x^9y^{19}) + h(a)x^{14}y^{14}$$

$$\text{where} \quad f(a) = 455(1 + a^2)(1 + 11a^2) \quad \text{and}$$

$$g(a) = 10010a(1 + a^2)(5 + 25a^2 + 11a^4 + a^6).$$

Miraculously, $f(i) = g(i) = 0$, and $h(i) = 5^7$. It follows that if $f_k(x, y) = \zeta_5^k x^2 + i\ x\ y + \zeta_5^{-k} y^2$ for $0 \le k \le 4$ and $f_5(x, y) = \sqrt{-5}\ x\ y$, then

$$\sum_{j=0}^{5} f_j^{14}(x, y) = 0. \tag{10}$$

By this time, you won't be surprised to hear me say that Felix Klein wouldn't have been surprised.

I don't know *why* (10) is true. Possible hint:

$$\sum_{j=0}^{5} f_j^{2k}(x,y) = 0 \quad \text{for} \quad k = 1,2,4$$

and $M_{6,1} = M_{6,2} = M_{6,4} = 0 \implies M_{6,7} = 0$.

The question is: *why* do the f_j^2's lie on this intersection?

Mark Green has shown that if r *entire* (let alone polynomial) functions ϕ_j satisfy $\sum_{j=1}^{r} \phi_j^N = 0$, then $N \le r(r-2)$; 14 is not that much less than 24, so this might well be an extremal example.

In 1884, Felix Klein wrote a famous book on the icosahedron, and he used an idea which seems to make plausible some of these identities. He first observed the Riemann sphere, which gives a 1-1 map of the unit sphere and the extended complex plane:

$$(a,b,c) \in S^2 \iff \frac{a+ib}{1-c} \in \mathbb{C}^*$$

$$u+iv \in \mathbb{C} \iff \left(\frac{2u}{u^2+v^2+1}, \frac{2v}{u^2+v^2+1}, \frac{u^2+v^2-1}{u^2+v^2+1}\right) \in S^2$$

The north pole corresponds to the point at infinity.

What Klein does now is associate a point on the sphere with a linear form in (x,y) whose "root" is the image of the point:

$$(a,b,c) \in S^2 \iff x - \left(\frac{a+ib}{1-c}\right) y, \quad , c \neq 1,$$

$$(0,0,1) \iff y.$$

Klein's goal was to start with a set of points of a regular polytope and take the product of the linear forms associated with its vertices. Linear changes of variable correspond to fractional linear changes in the roots:

$$p(x,y) = \mu \prod (x - \lambda_j y) \implies$$
$$p(ax+by, cx+dy) = \mu' \prod \left(x - \left(\frac{d\lambda_j - b}{a - c\lambda_j} \right) y \right).$$

Klein's goal was to start with a set of points of a regular polytope and take the product of the linear forms associated with its vertices. Linear changes of variable correspond to fractional linear changes in the roots:

$$p(x,y) = \mu \prod (x - \lambda_j y) \implies$$
$$p(ax+by, cx+dy) = \mu' \prod \left(x - \left(\frac{d\lambda_j - b}{a - c\lambda_j} \right) y \right).$$

Every rotation of the sphere corresponds to a change in variables of this product, though not every change in variables gives a rotation of the sphere. Since regular polytopes have many rotational symmetries, Klein found that the resulting polynomials has many symmetries as well.

Klein's goal was to start with a set of points of a regular polytope and take the product of the linear forms associated with its vertices. Linear changes of variable correspond to fractional linear changes in the roots:

$$p(x,y) = \mu \prod (x - \lambda_j y) \implies$$
$$p(ax+by, cx+dy) = \mu' \prod \left(x - \left(\frac{d\lambda_j - b}{a - c\lambda_j} \right) y \right).$$

Every rotation of the sphere corresponds to a change in variables of this product, though not every change in variables gives a rotation of the sphere. Since regular polytopes have many rotational symmetries, Klein found that the resulting polynomials has many symmetries as well.

Rather than taking the full product, look at antipodal pairs of vertices, leading to a quadratic form.

$$(a,b,c) \iff \frac{a+ib}{1-c} := re^{i\theta};$$
$$-(a,b,c) \iff -\frac{a+ib}{1+c} = -r^{-1}e^{i\theta}$$

and the resulting product

$$(x - re^{i\theta}y)(x + r^{-1}e^{i\theta}y) = x^2 - (r - r^{-1})e^{i\theta}xy - e^{2i\theta}y^2$$

is perfect for the sort of synching we've been doing. In particular, two antipodal regular d-gons parallel to the xy-plane yield the familiar-looking set of quadratics

$$\{\zeta_d^j \cdot (\zeta_d^{-j}x^2 - (r - r^{-1})xy - \zeta_d^j y^2) : 0 \le j \le d-1\}.$$

Here's what happens for the octahedron:

$$(\pm 1, 0, 0) \iff \pm 1 \iff x - y, x + y \iff x^2 - y^2$$
$$(0, \pm 1, 0) \iff \pm i \iff x - iy, x + iy \iff x^2 + y^2$$
$$(0, 0, \pm 1) \iff 0, \infty \iff x, y \iff xy$$

In other words, you get the Pythagorean parameterization (up to constants.)

Here's what happens for the octahedron:

$$(\pm 1, 0, 0) \iff \pm 1 \iff x - y, x + y \iff x^2 - y^2$$
$$(0, \pm 1, 0) \iff \pm i \iff x - iy, x + iy \iff x^2 + y^2$$
$$(0, 0, \pm 1) \iff 0, \infty \iff x, y \iff xy$$

In other words, you get the Pythagorean parameterization (up to constants.)
If you start with a cube with vertices at

$$\left(\pm\sqrt{\frac{2}{3}}, 0, \pm\sqrt{\frac{1}{3}}\right), \left(0, \pm\sqrt{\frac{2}{3}}, \pm\sqrt{\frac{1}{3}}\right)$$

you get the four Desboves-Elkies quadratics.

Here's what happens for the octahedron:

$$(\pm 1, 0, 0) \iff \pm 1 \iff x - y, x + y \iff x^2 - y^2$$
$$(0, \pm 1, 0) \iff \pm i \iff x - iy, x + iy \iff x^2 + y^2$$
$$(0, 0, \pm 1) \iff 0, \infty \iff x, y \iff xy$$

In other words, you get the Pythagorean parameterization (up to constants.)

If you start with a cube with vertices at

$$\left(\pm\sqrt{\frac{2}{3}}, 0, \pm\sqrt{\frac{1}{3}}\right), \left(0, \pm\sqrt{\frac{2}{3}}, \pm\sqrt{\frac{1}{3}}\right)$$

you get the four Desboves-Elkies quadratics.

And if you rotate the cube so that vertices are at the north and south poles, then you get the alternate formulation.

Six pairs of antipodal vertices of the icosahedron may be considered as the north/south poles and two rings of horizontal pentagons.

Six pairs of antipodal vertices of the icosahedron may be considered as the north/south poles and two rings of horizontal pentagons.

These give the sum of six quadratics to the 14th power equalling zero, and so far provide the best “reason” for their existence.

Six pairs of antipodal vertices of the icosahedron may be considered as the north/south poles and two rings of horizontal pentagons.

These give the sum of six quadratics to the 14th power equalling zero, and so far provide the best “reason” for their existence.

If you want to play with these ideas after the talk, the icosahedron can be rotated so the six pairs occur as two parallel sets of equilateral triangles. The golden ratio will show up in the associated identity.

Six pairs of antipodal vertices of the icosahedron may be considered as the north/south poles and two rings of horizontal pentagons.

These give the sum of six quadratics to the 14th power equalling zero, and so far provide the best “reason” for their existence.

If you want to play with these ideas after the talk, the icosahedron can be rotated so the six pairs occur as two parallel sets of equilateral triangles. The golden ratio will show up in the associated identity.

Many, many times.

Six pairs of antipodal vertices of the icosahedron may be considered as the north/south poles and two rings of horizontal pentagons.

These give the sum of six quadratics to the 14th power equalling zero, and so far provide the best “reason” for their existence.

If you want to play with these ideas after the talk, the icosahedron can be rotated so the six pairs occur as two parallel sets of equilateral triangles. The golden ratio will show up in the associated identity.

Many, many times.

The tetrahedron doesn’t have antipodal pairs of vertices.

Six pairs of antipodal vertices of the icosahedron may be considered as the north/south poles and two rings of horizontal pentagons.

These give the sum of six quadratics to the 14th power equalling zero, and so far provide the best "reason" for their existence.

If you want to play with these ideas after the talk, the icosahedron can be rotated so the six pairs occur as two parallel sets of equilateral triangles. The golden ratio will show up in the associated identity.

Many, many times.

The tetrahedron doesn't have antipodal pairs of vertices.

The dodecahedron gives 10 quadratics whose 14th powers are dependent. I don't know any *a priori* reason for the repeated appearance of "14".

Six pairs of antipodal vertices of the icosahedron may be considered as the north/south poles and two rings of horizontal pentagons.

These give the sum of six quadratics to the 14th power equalling zero, and so far provide the best "reason" for their existence.

If you want to play with these ideas after the talk, the icosahedron can be rotated so the six pairs occur as two parallel sets of equilateral triangles. The golden ratio will show up in the associated identity.

Many, many times.

The tetrahedron doesn't have antipodal pairs of vertices.

The dodecahedron gives 10 quadratics whose 14th powers are dependent. I don't know any *a priori* reason for the repeated appearance of "14".

I haven't found anything interesting yet for the quadratics based on the edges, or higher degree forms based on faces.

Here's (4) again:

$$\sum_{1\le i<j\le 4} (x_i + x_j)^4 + (x_i - x_j)^4 = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2.$$

This can be proved by noting that

$$(a + b)^4 + (a - b)^4 = 2a^4 + 12a^2b^2 + b^4$$

and counting the number of times a given monomial occurs on each side.

Here's (4) again:

$$\sum_{1 \le i < j \le 4} (x_i + x_j)^4 + (x_i - x_j)^4 = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2.$$

This can be proved by noting that

$$(a+b)^4 + (a-b)^4 = 2a^4 + 12a^2b^2 + b^4$$

and counting the number of times a given monomial occurs on each side.
Liouville used a version of this in 1859 to make the first advance on Waring's Problem since Lagrange's Four-Square Theorem.

Theorem

Every positive integer n is a sum of at most 53 4-th powers of integers.

Proof.

Write $n = t + 6m$, where $0 \le t \le 5$. By Lagrange, write $m = \sum_{i=1}^4 x_i^2$, and then write $x_i = \sum_{j=1}^4 y_{ij}^2$. Then

$$n = t + \sum_{i=1}^{4} 6(y_{i1}^2 + y_{i2}^2 + y_{i3}^2 + y_{i4}^2)^2$$

Proof.

Write $n = t + 6m$, where $0 \le t \le 5$. By Lagrange, write $m = \sum_{i=1}^4 x_i^2$, and then write $x_i = \sum_{j=1}^4 y_{ij}^2$. Then

$$n = t + \sum_{i=1}^{4} 6(y_{i1}^2 + y_{i2}^2 + y_{i3}^2 + y_{i4}^2)^2$$

Proof.

Write $n = t + 6m$, where $0 \le t \le 5$. By Lagrange, write $m = \sum_{i=1}^{4} x_i^2$, and then write $x_i = \sum_{j=1}^{4} y_{ij}^2$. Then

$$n = t + \sum_{i=1}^{4} 6(y_{i1}^2 + y_{i2}^2 + y_{i3}^2 + y_{i4}^2)^2$$

which by (4) is a sum of $t \le 5$ copies of 1^4 and 4×12 summands of the form $(y_{ij} \pm y_{ik})^4$. □

Proof.

Write $n = t + 6m$, where $0 \le t \le 5$. By Lagrange, write $m = \sum_{i=1}^{4} x_i^2$, and then write $x_i = \sum_{j=1}^{4} y_{ij}^2$. Then

$$n = t + \sum_{i=1}^{4} 6(y_{i1}^2 + y_{i2}^2 + y_{i3}^2 + y_{i4}^2)^2$$

which by (4) is a sum of $t \le 5$ copies of 1^4 and 4×12 summands of the form $(y_{ij} \pm y_{ik})^4$. □

For example, $1859 = 5 + 6 * 309 = 5 + 6 * (16^2 + 6^2 + 4^2 + 1^2)$ is one such representation, and after writing $16, 6, 4, 1$ each as a sum of squares, one is led to

$$1859 = 6 \cdot 4^4 + 2 \cdot 3^4 + 9 \cdot 2^4 + 17 \cdot 1^4 + 19 \cdot 0^4.$$

This is not the best way to study Waring's problem, and 53 is far from optimal. (For example, $1859 = 6^4 + 2 * 4^4 + 3 * 2^4 + 3 * 1^4$, with 9 cubes.)

This is not the best way to study Waring's problem, and 53 is far from optimal. (For example, $1859 = 6^4 + 2 * 4^4 + 3 * 2^4 + 3 * 1^4$, with 9 cubes.)
Mathematicians in the rest of the 19th century gave similar formulas for degrees 6, 8 and 10 and then, as usual, Hilbert destroyed their cottage industry when he solved Waring's Problem in 1909. A key step was this non-constructive theorem:

This is not the best way to study Waring's problem, and 53 is far from optimal. (For example, $1859 = 6^4 + 2 * 4^4 + 3 * 2^4 + 3 * 1^4$, with 9 cubes.)

Mathematicians in the rest of the 19th century gave similar formulas for degrees 6, 8 and 10 and then, as usual, Hilbert destroyed their cottage industry when he solved Waring's Problem in 1909. A key step was this non-constructive theorem:

Theorem

For all n, r, let $N = \binom{n+2r-1}{n-1}$. Then there exist $0 < \lambda_k \in \mathbb{Q}$ and $\alpha_{kj} \in \mathbb{Z}, 1 \le k \le N, 1 \le j \le n$, such that

$$\sum_{k=1}^{N} \lambda_k(\alpha_{k1}x_1 + \cdots + \alpha_{kn}x_n)^{2r} = (x_1^2 + \cdots + x_n^2)^r$$

The basic idea is of the proof to find the "average" $2r$-th power, where the coefficients range over the unit sphere S^{n-1}, by computing

$$F_{2r}(S^{n-1},\mu;x) := \int_{u\in S^{n-1}} (u_1x_1+\cdots+u_nx_n)^{2r}\,d\mu$$

where μ is the unit rotation-invariant measure.

The basic idea is of the proof to find the "average" $2r$-th power, where the coefficients range over the unit sphere S^{n-1}, by computing

$$F_{2r}(S^{n-1}, \mu; x) := \int_{u \in S^{n-1}} (u_1 x_1 + \cdots + u_n x_n)^{2r} d\mu$$

where μ is the unit rotation-invariant measure.
If $a, b \in \mathbb{R}^n$ and $||a|| = ||b||$, then by the rotational invariance, $F_{2r}(S^{n-1}, \mu; a) = F_{2r}(S^{n-1}, \mu; b)$.

The basic idea is of the proof to find the "average" $2r$-th power, where the coefficients range over the unit sphere S^{n-1}, by computing

$$F_{2r}(S^{n-1},\mu;x) := \int_{u\in S^{n-1}} (u_1x_1+\cdots+u_nx_n)^{2r}\,d\mu$$

where μ is the unit rotation-invariant measure.
If $a,b\in\mathbb{R}^n$ and $||a||=||b||$, then by the rotational invariance, $F_{2r}(S^{n-1},\mu;a)=F_{2r}(S^{n-1},\mu;b)$.
Thus $F_{2r}(S^{n-1},\mu;x)$ is a function of $||x||$ and since it is a form in the x_j's of degree $2r$,

$$F_{2r}(S^{n-1},\mu;x) = c_{n,r}(x_1^2+\cdots+x_n^2)^r$$

for some positive constant $c_{n,r}$. This constant can be computed by choosing x to be a unit vector and doing the integral.

The next step is approximate the integral with a Riemann sum and use Carathéodory's Theorem to show that each such sum can be replaced by one with at most N terms. Ultimately, an application Bolzano-Weierstrass gives a convergent subsequence. The argument that the coefficients are rational is subtle!

The next step is approximate the integral with a Riemann sum and use Carathéodory's Theorem to show that each such sum can be replaced by one with at most N terms. Ultimately, an application Bolzano-Weierstrass gives a convergent subsequence. The argument that the coefficients are rational is subtle!

It is sometimes convenient to ignore the algebraic constraints, and absorb the λ_k's into the powers by writing

$$(\beta_{k1}x_1 + \cdots + \beta_{kn}x_n)^{2r} = \lambda_k(\alpha_{k1}x_1 + \cdots + \alpha_{kn}x_n)^{2r}.$$

The rest of the talk will give some applications.

Suppose

$$\sum_{k=1}^{N} (\beta_{k1} x_1 + \cdots + \beta_{kn} x_n)^{2r} = (x_1^2 + \cdots + x_n^2)^r.$$

Suppose

$$\sum_{k=1}^{N} (\beta_{k1}x_1 + \cdots + \beta_{kn}x_n)^{2r} = (x_1^2 + \cdots + x_n^2)^r.$$

Dvoretzky's Theorem in functional analysis says that any infinite-dimensional Banach space contains isometric copies of every ℓ_2. Hilbert Identities can be used for concrete finite-dimensional examples. Bounds on the length of a Hilbert identity correspond to bound on the dimensions of the corresponding spaces.

For example, consider the vectors $u_j = (\beta_{1j}, \dots, \beta_{Nj}) \in \mathbb{R}^N$, $1 \le j \le n$. For any $x \in \mathbb{R}^n$, $|| \sum_j x_j u_j||_{2r}^{2r}$ is the left side, which by the right side is $||x||_2^{2r}$. In other words, the n-dimensional subspace $< u_j > \subset \ell_{2r}^N$ is isometric to ℓ_2^n.

Suppose a set S and non-negative measure μ are given. An *exact quadrature formula for* (S, μ) *of degree* d is an expression

$$\int_{u \in S} p(u)\ d\mu = \sum_{k=1}^{N} \lambda_k p(\alpha_k),$$

which holds for **all** forms p of degree d. (Conventionally, $\alpha_k \in S$ and $\lambda_k \geq 0$.)

Suppose a set S and non-negative measure μ are given. An *exact quadrature formula for* (S, μ) *of degree* d is an expression

$$\int_{u \in S} p(u)\ d\mu = \sum_{k=1}^{N} \lambda_k p(\alpha_k),$$

which holds for **all** forms p of degree d. (Conventionally, $\alpha_k \in S$ and $\lambda_k \geq 0$.)

Such an equation holds if and only if it holds for all monomials: $x^i = x_1^{i_1} \cdots x_n^{i_n}$ of degree d. Taken on the right hand side, we get the monomials in a sum of d-th powers of linear forms. It's getting kind of late in the talk, so I'll skip the derivation and get to the punch-line. I hope you trust me with the constants.

Theorem

Suppose μ *is the rotation-invariant unit measure on* S^{n-1} *and* $\lambda_k \in \mathbb{R}$, $\alpha_k \in \mathbb{R}^n$. *Then*

$$\int_{u \in S^{n-1}} p(u)\ d\mu = \sum_{k=1}^{N} \lambda_k p(\alpha_k),$$

is an exact quadrature formula of degree d *for* (S^{n-1}, μ) *iff*

$$\sum_{k=1}^{N} \lambda_k (\alpha_{k1} x_1 + \cdots + \alpha_{kn} x_n)^d = c_{n,d} (x_1^2 + \cdots + x_n^2)^{d/2},$$

where $c_{n,2r} = \prod_{j=1}^{r} \frac{n+2j}{1+2j}$ *and* $c_{n,2r+1} = 0$.

If q is a form of degree $d-2i$, then $(\sum x_j^2)^i q$ is a form of degree d which agrees with q on S^{n-1}, so an exact quadrature formula of degree d is also one of degree $d-2i$. If d is odd, the integral vanishes. By writing f as a sum of homogeneous pieces, we get

If q is a form of degree $d-2i$, then $(\sum x_j^2)^i q$ is a form of degree d which agrees with q on S^{n-1}, so an exact quadrature formula of degree d is also one of degree $d-2i$. If d is odd, the integral vanishes. By writing f as a sum of homogeneous pieces, we get

Corollary

If

$$\int_{u\in S^{n-1}} p(u)\ d\mu = \sum_{k=1}^{N} \lambda_k p(\alpha_k),$$

is an exact quadrature formula of degree d, then for **every** *polynomial f (homogeneous or not) of degree $\le 2\lfloor \frac{d}{2} \rfloor + 1$,*

$$\int_{u\in S^{n-1}} f(u)\ d\mu = \sum_{k=1}^{N} \frac{\lambda_k}{2}\big(f(\alpha_k) + f(-\alpha_k)\big)$$

These establish the centrality of Hilbert Identities for quadrature formulas on S^{n-1}. Another corollary uses an old ~~trick~~ method from numerical analysis.

Corollary

In any Hilbert Identity, $N \geq \binom{n+r-1}{n-1}$.

These establish the centrality of Hilbert Identities for quadrature formulas on S^{n-1}. Another corollary uses an old ~~trick~~ method from numerical analysis.

Corollary

In any Hilbert Identity, $N \geq \binom{n+r-1}{n-1}$.

Proof.

If $N < \binom{n+r-1}{r-1}$, then there exists a non-zero form h of degree r so that $h(\alpha_k) = 0$, $1 \leq k \leq N$. (Count the number of monomials.) Now put $p = h^2$ into the quadrature formula; we have

$$\int_{u \in S^{n-1}} h^2(u)\ d\mu = \sum_{k=1}^{N} \lambda_k h^2(\alpha_k),$$

which is > 0 on the left, and 0 on the right. Contradiction! ∎

How good an estimate is this? For $r = 2$ and $n = 4$, $\binom{2+4-1}{4-1} = 10$. Liouville's (4) has 12 terms. A while back, I proved that 10 is impossible, but 11 is possible:

$$12(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2$$

$$= 6(x_1 + x_2 + x_3 + x_4)^4 + \sum^{4}(x_2 \pm_1 x_3 \pm_2 x_4)^4 +$$

$$\sum^{2}(x_1 \pm \sqrt{2}x_2)^4 + \sum^{2}(x_1 \pm \sqrt{2}x_3)^4 + \sum^{2}(x_1 \pm \sqrt{2}x_4)^4.$$

The right-hand side is symmetric in $\{x_2, x_3, x_4\}$, but not in x_1.

How good an estimate is this? For $r = 2$ and $n = 4$, $\binom{2+4-1}{4-1} = 10$. Liouville's (4) has 12 terms. A while back, I proved that 10 is impossible, but 11 is possible:

$$12(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2$$

$$= 6(x_1 + x_2 + x_3 + x_4)^4 + \sum^{4}(x_2 \pm_1 x_3 \pm_2 x_4)^4 +$$

$$\sum^{2}(x_1 \pm \sqrt{2}x_2)^4 + \sum^{2}(x_1 \pm \sqrt{2}x_3)^4 + \sum^{2}(x_1 \pm \sqrt{2}x_4)^4.$$

The right-hand side is symmetric in $\{x_2, x_3, x_4\}$, but not in x_1.

I suspect this solution is unique, up to orthogonal changes of variable, but have been unable to prove it, in efforts spanning four different decades.

If a Hilbert Identity has minimal length, then the summands have some special properties

Corollary

If

$$\sum_{k=1}^{N} (\beta_{k1} x_1 + \cdots + \beta_{kn} x_n)^{2r} = (x_1^2 + \cdots + x_n^2)^r.$$

and $N = \binom{n+r-1}{n-1}$ *is minimal, then*

$$\left(\sum_{\ell=1}^{n} \beta_{k\ell}^2 \right)^r = \frac{1}{N} \prod_{j=1}^{r} \frac{n+2j}{1+2j}$$

is independent of k*.*

This leads to the final interpretation of Hilbert Identities. In a beautiful series of papers in the 1970s, Delsarte, Goethals and Seidel introduced the idea of the spherical design.

This leads to the final interpretation of Hilbert Identities. In a beautiful series of papers in the 1970s, Delsarte, Goethals and Seidel introduced the idea of the spherical design.

A set $X = \{v_1, \dots, v_N\} \in \mathbb{R}^n$ is a *spherical t-design* if for every polynomial $p(x_1, \dots, x_n)$, $\deg p \le t$, we have

$$\frac{\int_{S^{n-1}} f(x)\ d\mu}{\int_{S^{n-1}} d\mu} = \frac{1}{N} \sum_{j=1}^{N} f(v_j).$$

This leads to the final interpretation of Hilbert Identities. In a beautiful series of papers in the 1970s, Delsarte, Goethals and Seidel introduced the idea of the spherical design.

A set $X = \{v_1, \dots, v_N\} \in \mathbb{R}^n$ is a *spherical t-design* if for every polynomial $p(x_1, \dots, x_n)$, $\deg p \le t$, we have

$$\frac{\int_{S^{n-1}} f(x)\ d\mu}{\int_{S^{n-1}} d\mu} = \frac{1}{N} \sum_{j=1}^{N} f(v_j).$$

That is, the average of p on the sphere is equal to the average of p on these points: quadrature formulas with equal weights.

This leads to the final interpretation of Hilbert Identities. In a beautiful series of papers in the 1970s, Delsarte, Goethals and Seidel introduced the idea of the spherical design.

A set $X = \{v_1, \dots, v_N\} \in \mathbb{R}^n$ is a *spherical t-design* if for every polynomial $p(x_1, \dots, x_n)$, $\deg p \le t$, we have

$$\frac{\int_{S^{n-1}} f(x)\ d\mu}{\int_{S^{n-1}} d\mu} = \frac{1}{N}\sum_{j=1}^{N} f(v_j).$$

That is, the average of p on the sphere is equal to the average of p on these points: quadrature formulas with equal weights.

There are some wonderful theorems about spherical designs.

- The vertices of a regular d-gon are a spherical t-design in $\mathbb{R}^2$ if $d > t$.

- The vertices of a regular d-gon are a spherical t-design in $\mathbb{R}^2$ if $d > t$.
- For all (n, t), there exist spherical t-designs in $\mathbb{R}^n$.

- The vertices of a regular d-gon are a spherical t-design in $\mathbb{R}^2$ if $d > t$.
- For all (n, t), there exist spherical t-designs in $\mathbb{R}^n$.
- If $t = 2s$, then $N \ge \binom{n+s-1}{n-1} + \binom{n+s-2}{n-1}$; if $t = 2s+1$, then $N \ge 2\binom{n+s-1}{n-1}$, and there exists $N(n,t)$ so that for all $N \ge N(n,t)$, such a t-design with N points exists (Seymour and Zaslavsky).

- The vertices of a regular d-gon are a spherical t-design in $\mathbb{R}^2$ if $d > t$.
- For all (n, t), there exist spherical t-designs in $\mathbb{R}^n$.
- If $t = 2s$, then $N \geq \binom{n+s-1}{n-1} + \binom{n+s-2}{n-1}$; if $t = 2s + 1$, then $N \geq 2\binom{n+s-1}{n-1}$, and there exists $N(n, t)$ so that for all $N \geq N(n, t)$, such a t-design with N points exists (Seymour and Zaslavsky).
- If $d = 2s + 1$ and $N = 2\binom{n+s-1}{n-1}$, then X is called a *tight* spherical design. Such a tight spherical design must be antipodal and so its coefficients give a Hilbert Identity of minimal length.

- The vertices of a regular d-gon are a spherical t-design in $\mathbb{R}^2$ if $d > t$.
- For all (n, t), there exist spherical t-designs in $\mathbb{R}^n$.
- If $t = 2s$, then $N \geq \binom{n+s-1}{n-1} + \binom{n+s-2}{n-1}$; if $t = 2s+1$, then $N \geq 2\binom{n+s-1}{n-1}$, and there exists $N(n,t)$ so that for all $N \geq N(n,t)$, such a t-design with N points exists (Seymour and Zaslavsky).
- If $d = 2s+1$ and $N = 2\binom{n+s-1}{n-1}$, then X is called a *tight* spherical design. Such a tight spherical design must be antipodal and so its coefficients give a Hilbert Identity of minimal length.
- Your favorite symmetric pointset in $\mathbb{R}^n$ is a spherical design.

- The vertices of a regular d-gon are a spherical t-design in $\mathbb{R}^2$ if $d > t$.
- For all (n, t), there exist spherical t-designs in $\mathbb{R}^n$.
- If $t = 2s$, then $N \geq \binom{n+s-1}{n-1} + \binom{n+s-2}{n-1}$; if $t = 2s + 1$, then $N \geq 2\binom{n+s-1}{n-1}$, and there exists $N(n, t)$ so that for all $N \geq N(n, t)$, such a t-design with N points exists (Seymour and Zaslavsky).
- If $d = 2s + 1$ and $N = 2\binom{n+s-1}{n-1}$, then X is called a *tight* spherical design. Such a tight spherical design must be antipodal and so its coefficients give a Hilbert Identity of minimal length.
- Your favorite symmetric pointset in $\mathbb{R}^n$ is a spherical design.
- A tight spherical $2s + 1$-design in $\mathbb{R}^n$ defines the maximal number of lines through the origin in $\mathbb{R}^n$ which make only s different angles with each other.

- Tight spherical $2s+1$-designs exist whenever $n = 2$ and $2s+1 = 3$ and for $(2s+1, n) =$ (5,7), (5,23), (7,8), (7,23), (11,24). Otherwise, they are impossible unless $2s+1 = 5$ and $n = u^2 - 2$ (u odd) or $2s+1 = 7$ and $n = 3v^2 - 4$. Some non-existence results exist, but many cases remain open.

- Tight spherical $2s+1$-designs exist whenever $n=2$ and $2s+1=3$ and for $(2s+1,n) =$ (5,7), (5,23), (7,8), (7,23), (11,24). Otherwise, they are impossible unless $2s+1=5$ and $n=u^2-2$ (u odd) or $2s+1=7$ and $n=3v^2-4$. Some non-existence results exist, but many cases remain open.
- No new tight spherical designs have been found in the last 30 years. All known tight spherical designs are unique, up to rotation. All known proofs of this are *ad hoc*.

- Tight spherical $2s+1$-designs exist whenever $n = 2$ and $2s+1 = 3$ and for $(2s+1, n) =$ (5,7), (5,23), (7,8), (7,23), (11,24). Otherwise, they are impossible unless $2s+1 = 5$ and $n = u^2 - 2$ (u odd) or $2s+1 = 7$ and $n = 3v^2 - 4$. Some non-existence results exist, but many cases remain open.
- No new tight spherical designs have been found in the last 30 years. All known tight spherical designs are unique, up to rotation. All known proofs of this are *ad hoc*.
- Tight spherical designs lead to beautiful Hilbert Identities, as in (4). Take the indices below as cyclic mod 7, then

$$\sum_{i=1}^{7} \sum_{\pm} (x_i \pm x_{i+1} \pm x_{i+3})^4 = 12(x_1^2 + \cdots + x_7^2)^2.$$

This comes from the finite projective plane of order 2.

- The tight 11-design in $\mathbb{R}^{24}$ is derived from the minimal vectors in the Leech lattice and has the following hilarious implication. There is an isometric copy of ℓ_2^{24} in ℓ_{10}^{98280}, but not in ℓ_{10}^{98279}.

- The tight 11-design in $\mathbb{R}^{24}$ is derived from the minimal vectors in the Leech lattice and has the following hilarious implication. There is an isometric copy of ℓ_2^{24} in ℓ_{10}^{98280}, but not in ℓ_{10}^{98279}.
- Using the Schönemann coordinates for an icosahedron and letting $\Phi = \frac{\sqrt{5}+1}{2}$, so that $\Phi^4 + 1 = 3\Phi^2$, we have

$$6\Phi^2(x^2+y^2+z^2)^2 = (\Phi x + y)^4 + (\Phi x - y)^4 + (\Phi y + z)^4 + (\Phi y - z)^4 + (\Phi z + x)^4 + (\Phi z - x)^4.$$

Here's an identity which combines the previous discussion with most of your favorite small integers.

Theorem

If the equation

$$(x_1^2 + x_2^2 + x_3^2)^2 = \sum_{k=1}^{r} (a_k x_1 + b_k x_2 + c_k x_3)^4 \qquad (11)$$

holds, then $r \geq 6$. If $r = 6$, then this equation is true if and only if the 12 points $\pm(a_k, b_k, c_k)$ are the vertices of a regular icosahedron inscribed in a sphere with center 0 and radius $(5/6)^{1/4}$.

Here's an identity which combines the previous discussion with most of your favorite small integers.

Theorem

If the equation

$$(x_1^2 + x_2^2 + x_3^2)^2 = \sum_{k=1}^{r} (a_k x_1 + b_k x_2 + c_k x_3)^4 \qquad (12)$$

holds, then $r \geq 6$. *If* $r = 6$, *then this equation is true if and only if the 12 points* $\pm(a_k, b_k, c_k)$ *are the vertices of a regular icosahedron inscribed in a sphere with center 0 and radius* $(5/6)^{1/4}$.

References

For (1) and (4):

- Dickson, L. E., History of the Theory of Numbers, v.2., AMS (1920, 1966)

References

For (1) and (4):

- Dickson, L. E., History of the Theory of Numbers, v.2., AMS (1920, 1966)
- Friedman, A., Mean values and polyharmonic polynomials, Michigan Math. J. 4 (1957), 137–145

References

For (1) and (4):

- Dickson, L. E., History of the Theory of Numbers, v.2., AMS (1920, 1966)
- Friedman, A., Mean values and polyharmonic polynomials, Michigan Math. J. 4 (1957), 137–145
- Ellison, W. J., Waring's problem, Amer. Math. Monthly 78 (1971), no. 1, 10–36

References

For (1) and (4):

- Dickson, L. E., History of the Theory of Numbers, v.2., AMS (1920, 1966)
- Friedman, A., Mean values and polyharmonic polynomials, Michigan Math. J. 4 (1957), 137–145
- Ellison, W. J., Waring's problem, Amer. Math. Monthly 78 (1971), no. 1, 10–36
- Delsarte, P, Goethals, J.-M., Seidel, J. J., Spherical codes and designs, Geometriae Dedicata 6 (1977), no. 3, 363–388, and many others

References

For (1) and (4):

- Dickson, L. E., History of the Theory of Numbers, v.2., AMS (1920, 1966)
- Friedman, A., Mean values and polyharmonic polynomials, Michigan Math. J. 4 (1957), 137–145
- Ellison, W. J., Waring's problem, Amer. Math. Monthly 78 (1971), no. 1, 10–36
- Delsarte, P, Goethals, J.-M., Seidel, J. J., Spherical codes and designs, Geometriae Dedicata 6 (1977), no. 3, 363–388, and many others
- Sums of even powers of real linear forms, Mem. AMS, No. 463, 1992

References

For (2):

References

For (2):

- Viète, F., The Analytic Art, translated by T. Richard Witmer (1591, 1983)

References

For (2):

- Viète, F., The Analytic Art, translated by T. Richard Witmer (1591, 1983)
- (with J. Rouse) On the sums of two cubes, to appear in the Int. J. Number Theory, available at the arXiv: 1012.5801 or www.math.uiuc.edu/∼reznick/cubic13111f.pdf

References

For (2):

- Viète, F., The Analytic Art, translated by T. Richard Witmer (1591, 1983)
- (with J. Rouse) On the sums of two cubes, to appear in the Int. J. Number Theory, available at the arXiv: 1012.5801 or www.math.uiuc.edu/∼reznick/cubic13111f.pdf

References

For (2):

- Viète, F., The Analytic Art, translated by T. Richard Witmer (1591, 1983)
- (with J. Rouse) On the sums of two cubes, to appear in the Int. J. Number Theory, available at the arXiv: 1012.5801 or www.math.uiuc.edu/∼reznick/cubic13111f.pdf

For (3):

References

For (2):

- Viète, F., The Analytic Art, translated by T. Richard Witmer (1591, 1983)
- (with J. Rouse) On the sums of two cubes, to appear in the Int. J. Number Theory, available at the arXiv: 1012.5801 or www.math.uiuc.edu/∼reznick/cubic13111f.pdf

For (3):

- Klein, Felix, Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom 5ten Grade (1884); English Translation: Lectures on the Icosahedron; and the Solution of Equations of the Fifth Degree (1914)

References

For (2):

- Viète, F., The Analytic Art, translated by T. Richard Witmer (1591, 1983)
- (with J. Rouse) On the sums of two cubes, to appear in the Int. J. Number Theory, available at the arXiv: 1012.5801 or www.math.uiuc.edu/∼reznick/cubic13111f.pdf

For (3):

- Klein, Felix, Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom 5ten Grade (1884); English Translation: Lectures on the Icosahedron; and the Solution of Equations of the Fifth Degree (1914)
- Patterns of dependence among powers of polynomials, DIMACS Ser. in Discrete Mathematics and Theoretical Computer Science, 60 (2003), 101-121