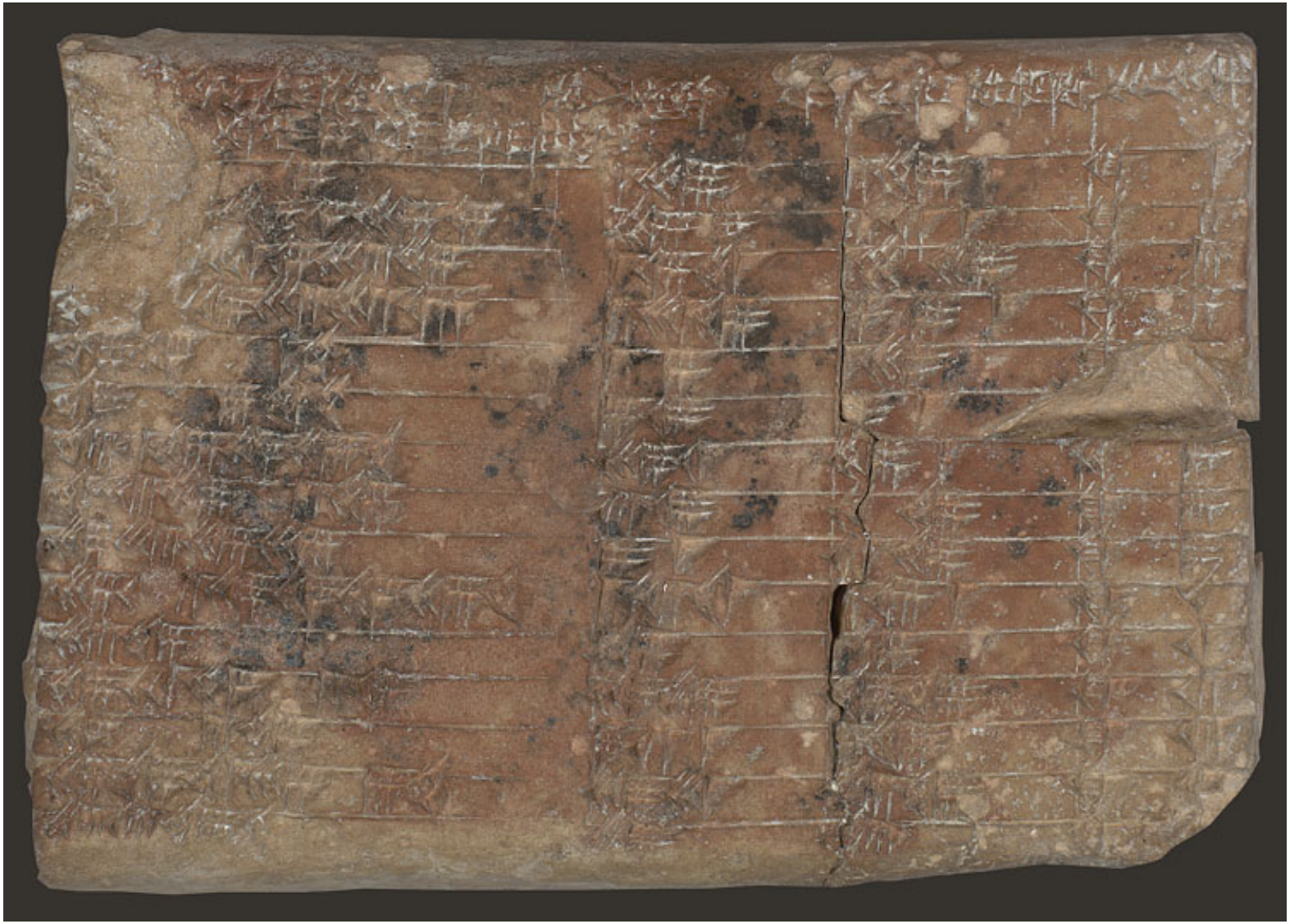
Auxiliary structures in number theory

Kiran S. Kedlaya

Department of Mathematics
University of California, San Diego
kedlaya@ucsd.edu
http://kskedlaya.org/slides/

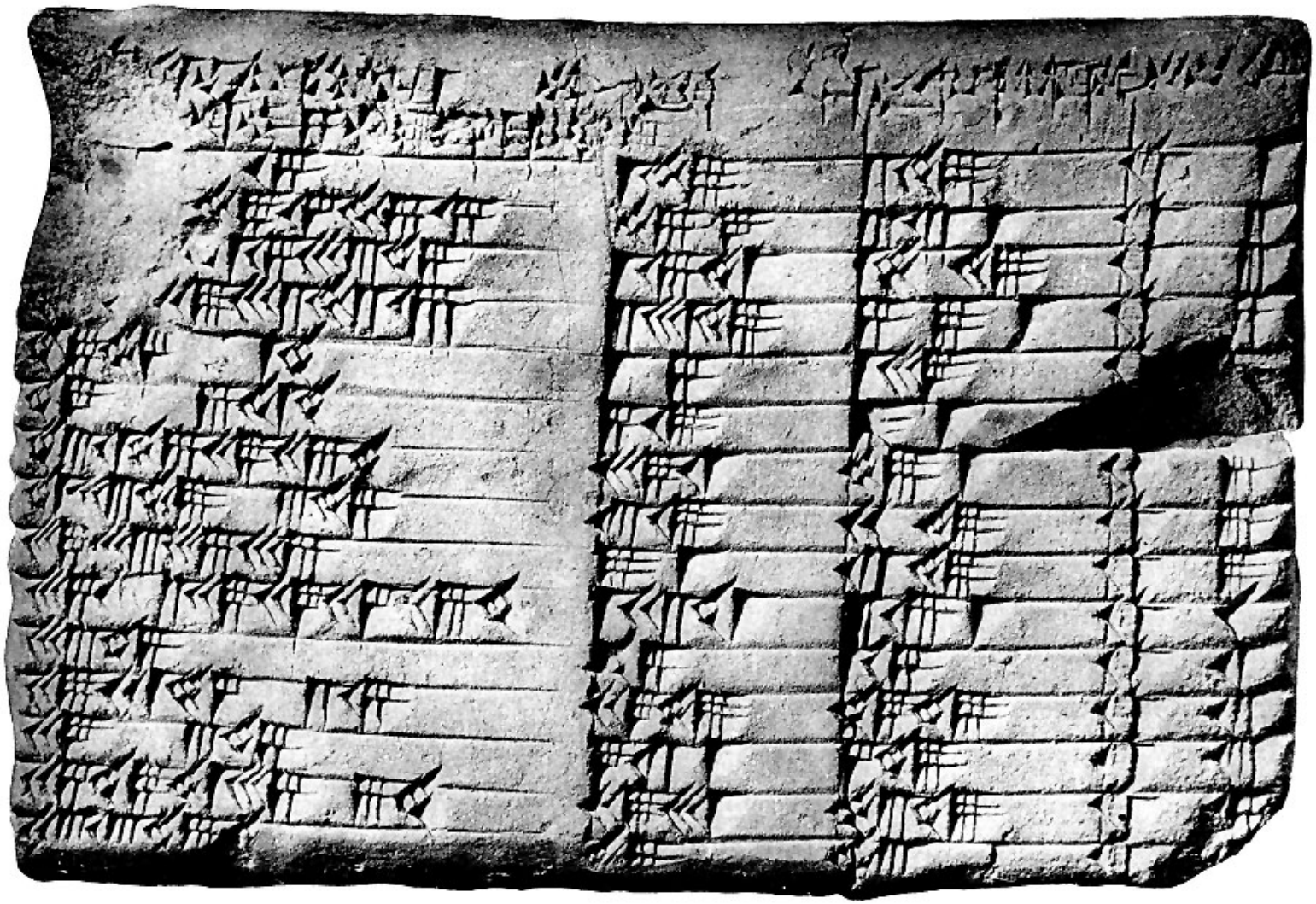
Symposium for Undergraduates in the Mathematical Sciences
Brown University
March 12, 2016

The Plimpton 322 tablet (Babylonian, c. 1800 BCE)



Columbia University Libraries, http://www.columbia.edu/cu/lweb/eresources/exhibitions/treasures/html/158.html

Another view of Plimpton 322



This photo, and the following analysis, are taken from a web site of Bill Casselman (University of British Columbia): `http://www.math.ubc.ca/~cass/courses/m446-03/pl322/pl322.html`.

Plimpton 322 and Pythagorean triples

This tablet is a table of numbers in base 60; the symbols

represent $1, \ldots, 9$ and $10, \ldots, 50$. (There is no symbol to represent zero!)

According to Neugebauer and Sachs (1945), the tablet is a computation of some *Pythagorean triples* using the method we know from Euclid: form

$$(m(p^2 - q^2), 2mpq, m(p^2 + q^2))$$

for various $p, q, m \in \mathbb{Z}$ with $p > q > 0$, $\gcd(p, q) = 1$, and pq even.

E.g., the first row takes $m = 1, p = 12, q = 5$ to obtain

$$119^2 + 120^2 = 14161 + 14400 = 28561 = 169^2.$$

Plimpton 322 and Pythagorean triples

This tablet is a table of numbers in base 60; the symbols

represent $1, \ldots, 9$ and $10, \ldots, 50$. (There is no symbol to represent zero!)

According to Neugebauer and Sachs (1945), the tablet is a computation of some *Pythagorean triples* using the method we know from Euclid: form

$$(m(p^2 - q^2), 2mpq, m(p^2 + q^2))$$

for various $p, q, m \in \mathbb{Z}$ with $p > q > 0$, $\gcd(p, q) = 1$, and pq even.

E.g., the first row takes $m = 1, p = 12, q = 5$ to obtain

$$119^2 + 120^2 = 14161 + 14400 = 28561 = 169^2.$$

Plimpton 322 and Pythagorean triples

This tablet is a table of numbers in base 60; the symbols

represent $1, \ldots, 9$ and $10, \ldots, 50$. (There is no symbol to represent zero!)

According to Neugebauer and Sachs (1945), the tablet is a computation of some *Pythagorean triples* using the method we know from Euclid: form

$$(m(p^2 - q^2), 2mpq, m(p^2 + q^2))$$

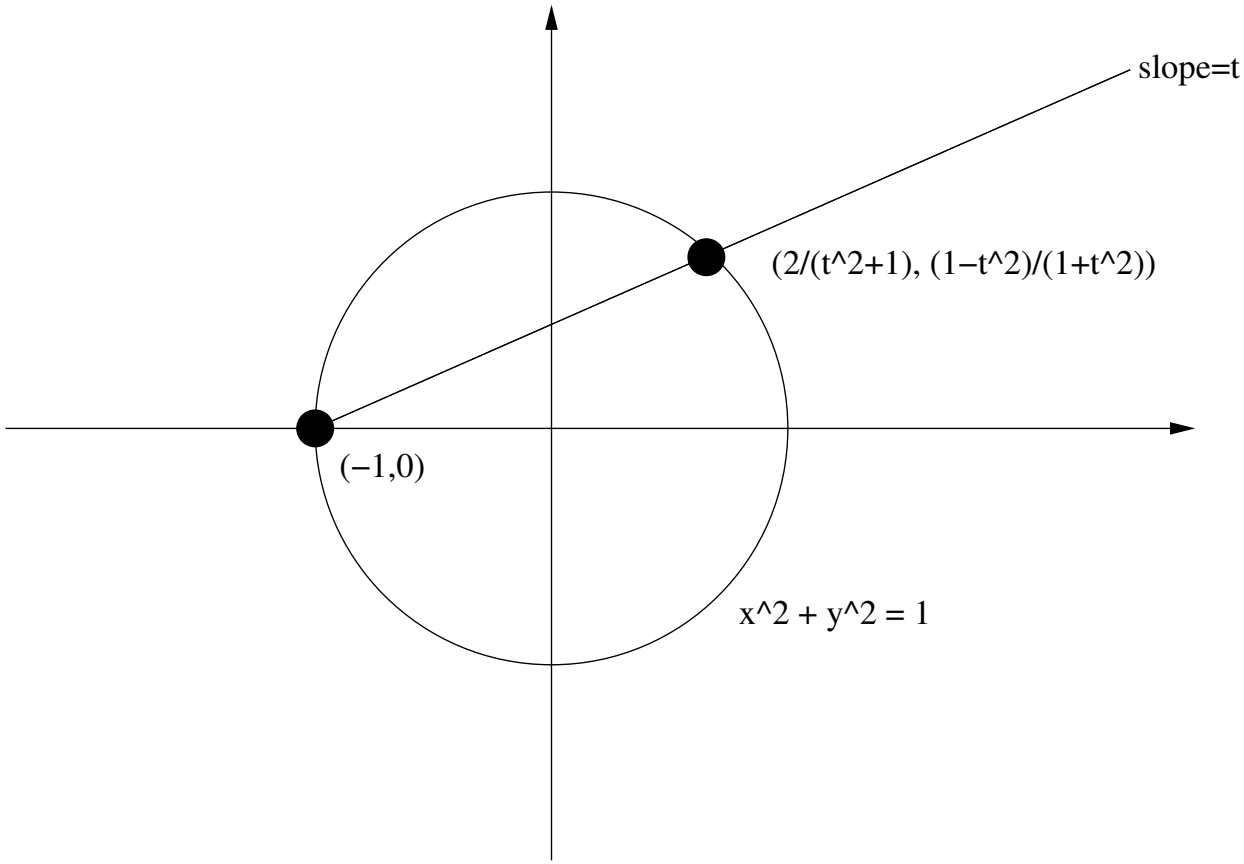
for various $p, q, m \in \mathbb{Z}$ with $p > q > 0$, $\gcd(p, q) = 1$, and pq even.

E.g., the first row takes $m = 1, p = 12, q = 5$ to obtain

$$119^2 + 120^2 = 14161 + 14400 = 28561 = 169^2.$$

An auxiliary structure in Pythagorean triples

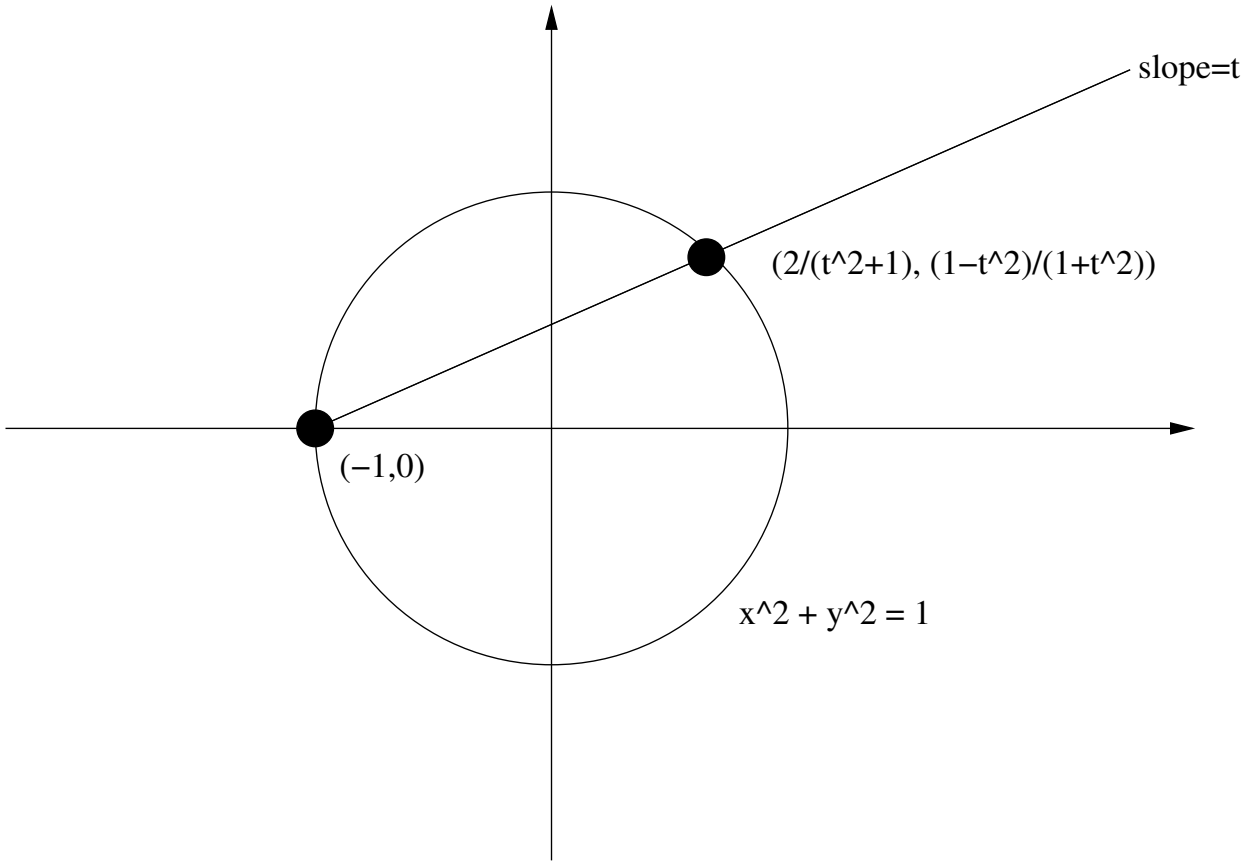
A geometric interpretation of Euclid's method via *stereographic projection*:



A line with rational slope through one rational point has rational coefficients, so its second intersection with the circle is again rational.

An auxiliary structure in Pythagorean triples

A geometric interpretation of Euclid's method via *stereographic projection*:



A line with rational slope through one rational point has rational coefficients, so its second intersection with the circle is again rational.

An example of Diophantos

The *Arithmetica* of Diophantos (3rd century CE) is the first known treatise on the solution of algebraic equations in integers or rational numbers. For this reason, such equations are commonly called as *Diophantine equations*.

Example (Book IV, Problem 24): To divide a given number into two numbers such that their product is a cube minus its side.

In other words, given a, find x and y such that

$$y(a-y) = x^3 - x.$$

The following analysis, and illustration, are from: Ezra Brown and Bruce T. Myers, Elliptic curves from Mordell to Diophantus and back, *American Math. Monthly* **109** (2002), 639–649.

An example of Diophantos

The *Arithmetica* of Diophantos (3rd century CE) is the first known treatise on the solution of algebraic equations in integers or rational numbers. For this reason, such equations are commonly called as *Diophantine equations*.

Example (Book IV, Problem 24): To divide a given number into two numbers such that their product is a cube minus its side.

In other words, given a, find x and y such that

$$y(a-y) = x^3 - x.$$

The following analysis, and illustration, are from: Ezra Brown and Bruce T. Myers, Elliptic curves from Mordell to Diophantus and back, *American Math. Monthly* **109** (2002), 639–649.

An example of Diophantos

The *Arithmetica* of Diophantos (3rd century CE) is the first known treatise on the solution of algebraic equations in integers or rational numbers. For this reason, such equations are commonly called as *Diophantine equations*.

Example (Book IV, Problem 24): To divide a given number into two numbers such that their product is a cube minus its side.

In other words, given a, find x and y such that

$$y(a-y) = x^3 - x.$$

The following analysis, and illustration, are from: Ezra Brown and Bruce T. Myers, Elliptic curves from Mordell to Diophantus and back, *American Math. Monthly* **109** (2002), 639–649.

An example of Diophantos

The *Arithmetica* of Diophantos (3rd century CE) is the first known treatise on the solution of algebraic equations in integers or rational numbers. For this reason, such equations are commonly called as *Diophantine equations*.

Example (Book IV, Problem 24): To divide a given number into two numbers such that their product is a cube minus its side.

In other words, given a, find x and y such that

$$y(a-y) = x^3 - x.$$

The following analysis, and illustration, are from: Ezra Brown and Bruce T. Myers, Elliptic curves from Mordell to Diophantus and back, *American Math. Monthly* **109** (2002), 639–649.

An example of Diophantos (continued)

For any a, there is a trivial solution $(-1, 0)$. As in the previous example, let's try to generate a new solution by solving the equation

$$t(x+1)(a - t(x+1)) = x^3 - x.$$

For any given t, this is a cubic polynomial with $x = -1$ as one root, so there is no reason for the other two roots to be rational.

However, if we choose t so that $x = -1$ occurs as a *double* root, then the third root will be forced to be rational. This occurs for $t = 2/a$.

Note: Diophantos did not have the language of algebra, so he was forced to illustrate his methods in terms of "typical" values of a. In this case he used $a = 6$, in which case this procedure yields

$$(x, y) = (17/9, 26/27).$$

An example of Diophantos (continued)

For any a, there is a trivial solution $(-1, 0)$. As in the previous example, let's try to generate a new solution by solving the equation

$$t(x+1)(a - t(x+1)) = x^3 - x.$$

For any given t, this is a cubic polynomial with $x = -1$ as one root, so there is no reason for the other two roots to be rational.

However, if we choose t so that $x = -1$ occurs as a *double* root, then the third root will be forced to be rational. This occurs for $t = 2/a$.

Note: Diophantos did not have the language of algebra, so he was forced to illustrate his methods in terms of "typical" values of a. In this case he used $a = 6$, in which case this procedure yields

$$(x, y) = (17/9, 26/27).$$

An example of Diophantos (continued)

For any a, there is a trivial solution $(-1, 0)$. As in the previous example, let's try to generate a new solution by solving the equation

$$t(x+1)(a - t(x+1)) = x^3 - x.$$

For any given t, this is a cubic polynomial with $x = -1$ as one root, so there is no reason for the other two roots to be rational.

However, if we choose t so that $x = -1$ occurs as a *double* root, then the third root will be forced to be rational. This occurs for $t = 2/a$.

Note: Diophantos did not have the language of algebra, so he was forced to illustrate his methods in terms of "typical" values of a. In this case he used $a = 6$, in which case this procedure yields

$$(x, y) = (17/9, 26/27).$$

An example of Diophantos (continued)

For any a, there is a trivial solution $(-1, 0)$. As in the previous example, let's try to generate a new solution by solving the equation

$$t(x+1)(a - t(x+1)) = x^3 - x.$$

For any given t, this is a cubic polynomial with $x = -1$ as one root, so there is no reason for the other two roots to be rational.

However, if we choose t so that $x = -1$ occurs as a *double* root, then the third root will be forced to be rational. This occurs for $t = 2/a$.

Note: Diophantos did not have the language of algebra, so he was forced to illustrate his methods in terms of "typical" values of a. In this case he used $a = 6$, in which case this procedure yields

$$(x, y) = (17/9, 26/27).$$

Context: elliptic curves

This example went unexplained for over 1000 years, until similar examples began to be considered by Fermat (17th century), e.g.,

$$x^3 + y^3 = 1$$

which only has the solutions $(0, 1), (1, 0)$. In this case, the double root trick fails because starting with either solution, forcing the double root automatically forces a *triple* root.

The ultimate explanation is that for certain curves in the plane (called *elliptic curves*), the points[1] have a natural *addition law* with O as the identity element. This law is commutative, associative, and admits inverses, so one gets an *abelian group* structure. The method of Diophantos amounts to *doubling* a point, i.e., adding it to itself.

[1] One must be careful here about points at infinity.

Context: elliptic curves

This example went unexplained for over 1000 years, until similar examples began to be considered by Fermat (17th century), e.g.,

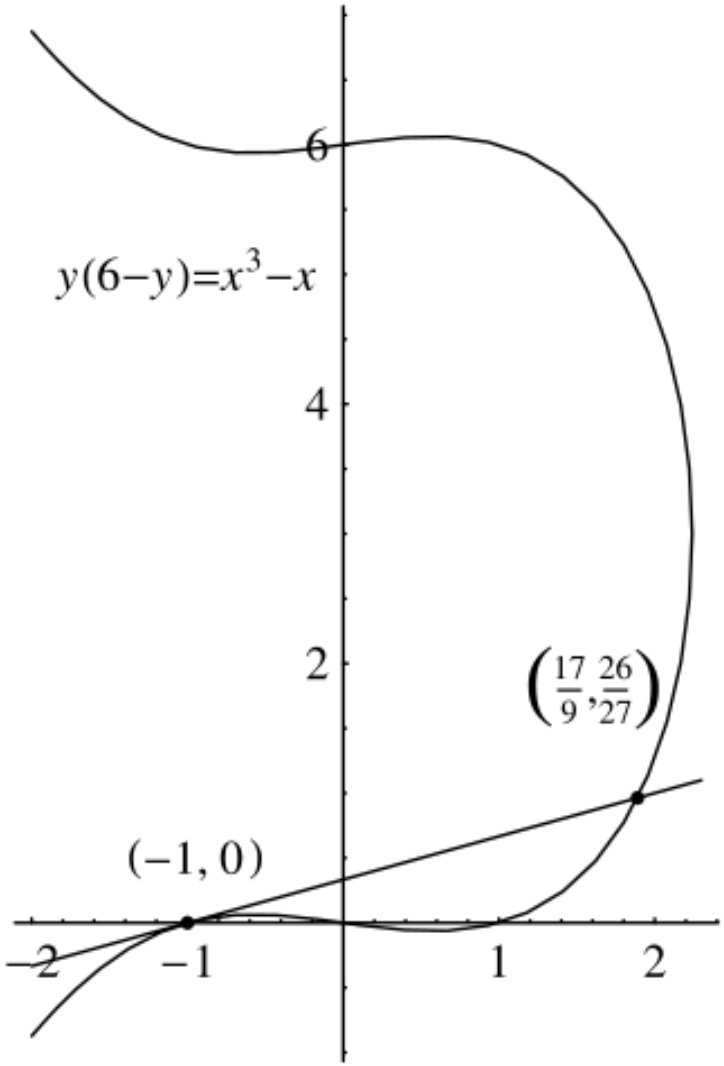
$$x^3 + y^3 = 1$$

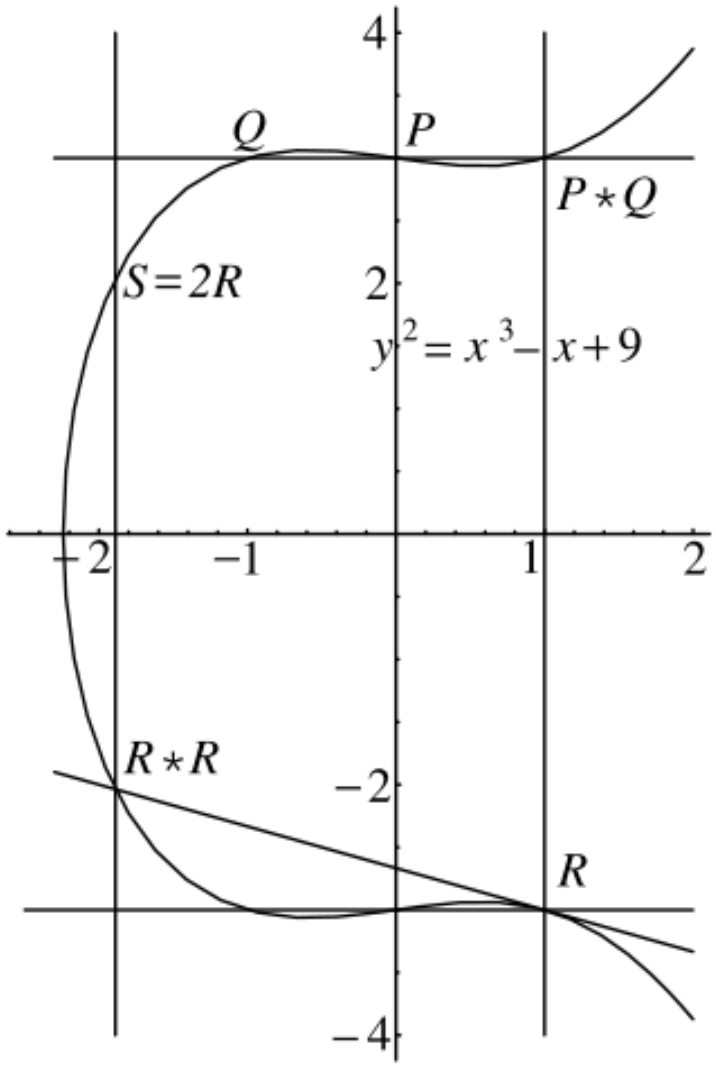
which only has the solutions $(0, 1), (1, 0)$. In this case, the double root trick fails because starting with either solution, forcing the double root automatically forces a *triple* root.

The ultimate explanation is that for certain curves in the plane (called *elliptic curves*), the points[1] have a natural *addition law* with O as the identity element. This law is commutative, associative, and admits inverses, so one gets an *abelian group* structure. The method of Diophantos amounts to *doubling* a point, i.e., adding it to itself.

[1] One must be careful here about points at infinity.

Illustration: elliptic curves





Aside: elliptic curves in computer science

As an aside, I note that elliptic curves have recently become of great value not just for mathematicians, but also for computer scientists.

- Elliptic curves give rise to a good method of factoring large integers, particularly[2] when one prime factor is smaller than the others, but is still too large to be found by trial division.
- Elliptic curves also give rise to public-key cryptography techniques which are widely used in practice (e.g., SSL, digital signatures, Bitcoin).

There are also applications of more sophisticated geometric objects like *hyperelliptic curves*

$$y^2 = (\text{polynomial in } x).$$

[2] This is not the case for the moduli used in RSA cryptography, which are products of two similarly large primes. However, factorization techniques like the number field sieve involve some auxiliary factorizations to which elliptic curves do apply.

Aside: elliptic curves in computer science

As an aside, I note that elliptic curves have recently become of great value not just for mathematicians, but also for computer scientists.

- Elliptic curves give rise to a good method of factoring large integers, particularly[2] when one prime factor is smaller than the others, but is still too large to be found by trial division.
- Elliptic curves also give rise to public-key cryptography techniques which are widely used in practice (e.g., SSL, digital signatures, Bitcoin).

There are also applications of more sophisticated geometric objects like *hyperelliptic curves*

$$y^2 = (\text{polynomial in } x).$$

[2] This is not the case for the moduli used in RSA cryptography, which are products of two similarly large primes. However, factorization techniques like the number field sieve involve some auxiliary factorizations to which elliptic curves do apply.

Aside: elliptic curves in computer science

As an aside, I note that elliptic curves have recently become of great value not just for mathematicians, but also for computer scientists.

- Elliptic curves give rise to a good method of factoring large integers, particularly[2] when one prime factor is smaller than the others, but is still too large to be found by trial division.
- Elliptic curves also give rise to public-key cryptography techniques which are widely used in practice (e.g., SSL, digital signatures, Bitcoin).

There are also applications of more sophisticated geometric objects like *hyperelliptic curves*

$$y^2 = (\text{polynomial in } x).$$

[2] This is not the case for the moduli used in RSA cryptography, which are products of two similarly large primes. However, factorization techniques like the number field sieve involve some auxiliary factorizations to which elliptic curves do apply.

What is arithmetic geometry?

The kind of auxiliary structures we have seen so far are objects of *algebraic geometry*. Classical algebraic geometry takes place over an algebraically closed field (e.g., $\mathbb{C}$); working over $\mathbb{Q}$ typically requires extra techniques of *arithmetic geometry*.

For example, any two conic curves over $\mathbb{C}$ are isomorphic. But over $\mathbb{Q}$, this only holds for conic curves containing *at least one* rational point; reasons[3] for failure can be for "archimedean" (e.g., $x^2 + y^2 = -1$, due to $\mathbb{R}$) or "p-adic" (e.g., $x^2 + y^2 = 3$, due to congruences mod 4).

[3] For conics, there are no other modes of failure; this is part of the *Hasse-Minkowski theorem*. This is special to conics; for instance, Selmer discovered that $3x^3 + 4y^3 = -5$ has no $\mathbb{Q}$-points, but not for any archimedean or p-adic reason.

What is arithmetic geometry?

The kind of auxiliary structures we have seen so far are objects of *algebraic geometry*. Classical algebraic geometry takes place over an algebraically closed field (e.g., $\mathbb{C}$); working over $\mathbb{Q}$ typically requires extra techniques of *arithmetic geometry*.

For example, any two conic curves over $\mathbb{C}$ are isomorphic. But over $\mathbb{Q}$, this only holds for conic curves containing *at least one* rational point; reasons[3] for failure can be for "archimedean" (e.g., $x^2 + y^2 = -1$, due to $\mathbb{R}$) or "p-adic" (e.g., $x^2 + y^2 = 3$, due to congruences mod 4).

[3] For conics, there are no other modes of failure; this is part of the *Hasse-Minkowski theorem*. This is special to conics; for instance, Selmer discovered that $3x^3 + 4y^3 = -5$ has no $\mathbb{Q}$-points, but not for any archimedean or p-adic reason.

What is arithmetic geometry?

The kind of auxiliary structures we have seen so far are objects of *algebraic geometry*. Classical algebraic geometry takes place over an algebraically closed field (e.g., $\mathbb{C}$); working over $\mathbb{Q}$ typically requires extra techniques of *arithmetic geometry*.

For example, any two conic curves over $\mathbb{C}$ are isomorphic. But over $\mathbb{Q}$, this only holds for conic curves containing *at least one* rational point; reasons[3] for failure can be for "archimedean" (e.g., $x^2 + y^2 = -1$, due to $\mathbb{R}$) or "p-adic" (e.g., $x^2 + y^2 = 3$, due to congruences mod 4).

[3] For conics, there are no other modes of failure; this is part of the *Hasse-Minkowski theorem*. This is special to conics; for instance, Selmer discovered that $3x^3 + 4y^3 = -5$ has no $\mathbb{Q}$-points, but not for any archimedean or p-adic reason.

A problem outside arithmetic geometry

One problem that historically resisted many advances of arithmetic geometry is *Fermat's last theorem*: for any integer $n \geq 3$, the equation

$$x^n + y^n = 1$$

has no rational solutions with $xy \neq 0$.

For any individual n, one can try to use geometric techniques to study this equation. (For example, Fermat himself gave a proof for $n = 4$, which means that hereafter one need only worry about n prime.) However, it is very hard to use this approach to get a statement uniformly over n.

A problem outside arithmetic geometry

One problem that historically resisted many advances of arithmetic geometry is *Fermat's last theorem*: for any integer $n \geq 3$, the equation

$$x^n + y^n = 1$$

has no rational solutions with $xy \neq 0$.

For any individual n, one can try to use geometric techniques to study this equation. (For example, Fermat himself gave a proof for $n = 4$, which means that hereafter one need only worry about n prime.) However, it is very hard to use this approach to get a statement uniformly over n.

The Frey-Hellegouarc'h curve

An alternate approach was discovered by Hellegouarc'h (1975): to try to rule out the existence of a nontrivial integer solution of $A^n + B^n = C^n$, look at the elliptic curve

$$y^2 = x(x - A^n)(x + B^n).$$

Frey (1982) realized that such a curve, were it to exist, would have very strange properties. For example, there are "too few" primes for which the reduction of this equation modulo p behaves badly (i.e., the curve acquires a singularity because two of the roots of the polynomial in x come together).

The Frey-Hellegouarc'h curve

An alternate approach was discovered by Hellegouarc'h (1975): to try to rule out the existence of a nontrivial integer solution of $A^n + B^n = C^n$, look at the elliptic curve

$$y^2 = x(x - A^n)(x + B^n).$$

Frey (1982) realized that such a curve, were it to exist, would have very strange properties. For example, there are "too few" primes for which the reduction of this equation modulo p behaves badly (i.e., the curve acquires a singularity because two of the roots of the polynomial in x come together).

The Frey-Hellegouarc'h curve (continued)

Again, associate to a solution of $A^n + B^n = C^n$ the elliptic curve

$$y^2 = x(x - A^n)(x + B^n).$$

Serre (1985) made Frey's intuition precise, in the form of a conjecture proved by Ribet (1990): the existence of a Frey-Hellegouarc'h curve is inconsistent with the existence of a corresponding *modular form*.

That existence had itself been conjectured based on work of Taniyama, Shimura, and Weil. That conjecture was proved (in sufficient cases) by Wiles and Taylor-Wiles (1995), thus resolving Fermat's last theorem once and for all.

To say more, let us back up a few years...

The Frey-Hellegouarc'h curve (continued)

Again, associate to a solution of $A^n + B^n = C^n$ the elliptic curve

$$y^2 = x(x - A^n)(x + B^n).$$

Serre (1985) made Frey's intuition precise, in the form of a conjecture proved by Ribet (1990): the existence of a Frey-Hellegouarc'h curve is inconsistent with the existence of a corresponding *modular form*.

That existence had itself been conjectured based on work of Taniyama, Shimura, and Weil. That conjecture was proved (in sufficient cases) by Wiles and Taylor-Wiles (1995), thus resolving Fermat's last theorem once and for all.

To say more, let us back up a few years...

The Frey-Hellegouarc'h curve (continued)

Again, associate to a solution of $A^n + B^n = C^n$ the elliptic curve

$$y^2 = x(x - A^n)(x + B^n).$$

Serre (1985) made Frey's intuition precise, in the form of a conjecture proved by Ribet (1990): the existence of a Frey-Hellegouarc'h curve is inconsistent with the existence of a corresponding *modular form*.

That existence had itself been conjectured based on work of Taniyama, Shimura, and Weil. That conjecture was proved (in sufficient cases) by Wiles and Taylor-Wiles (1995), thus resolving Fermat's last theorem once and for all.

To say more, let us back up a few years...

The Frey-Hellegouarc'h curve (continued)

Again, associate to a solution of $A^n + B^n = C^n$ the elliptic curve

$$y^2 = x(x - A^n)(x + B^n).$$

Serre (1985) made Frey's intuition precise, in the form of a conjecture proved by Ribet (1990): the existence of a Frey-Hellegouarc'h curve is inconsistent with the existence of a corresponding *modular form*.

That existence had itself been conjectured based on work of Taniyama, Shimura, and Weil. That conjecture was proved (in sufficient cases) by Wiles and Taylor-Wiles (1995), thus resolving Fermat's last theorem once and for all.

To say more, let us back up a few years...

Generating functions

Given a sequence of integers $a_0, a_1, \ldots$, the associated *generating function* is the power series

$$a_0 + a_1 q + a_2 q^2 + \cdots .$$

In many cases, this series converges and the properties of the resulting function give a lot of useful control on the original sequence.

For example, Euler (mid-1700s) observed that the power series

$$(1-q)^{-1}(1-q^2)^{-1}\cdots$$

is the generating function for the sequence counting *partitions* of n, i.e., ways to write n as an unordered sum of positive integers. (For instance, there are 7 partitions of 5: $1+1+1+1+1$, $1+1+1+2$, $1+2+2$, $1+1+3$, $1+4$, $2+3$, 5.)

Generating functions

Given a sequence of integers $a_0, a_1, \ldots$, the associated *generating function* is the power series

$$a_0 + a_1 q + a_2 q^2 + \cdots .$$

In many cases, this series converges and the properties of the resulting function give a lot of useful control on the original sequence.

For example, Euler (mid-1700s) observed that the power series

$$(1-q)^{-1}(1-q^2)^{-1}\cdots$$

is the generating function for the sequence counting *partitions* of n, i.e., ways to write n as an unordered sum of positive integers. (For instance, there are 7 partitions of 5: $1+1+1+1+1$, $1+1+1+2$, $1+2+2$, $1+1+3$, $1+4$, $2+3$, 5.)

Analytic properties of generating functions

Some deep links between combinatorial generating functions and complex analysis were discovered by Legendre, Abel, and Jacobi (1820s). This was a bit of an accident: they were trying to understand the integrals that come up when trying to compute arclengths on an ellipse.[4]

This theory was further developed by Weierstrass (1860s). One key example is the *discriminant modular form*

$$\Delta(q) = q \prod_{n=1}^{\infty} (1-q^n)^{24},$$

which has a strong symmetry property: for $q = e^{2\pi i \tau}$ with $\mathrm{Im}(\tau) > 0$ and $a, b, c, d \in \mathbb{Z}$ with $ad - bc = 1$,

$$\Delta\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{12} \Delta(\tau)$$

[4] These are closely related to *elliptic curves*, whence that terminology.

Analytic properties of generating functions

Some deep links between combinatorial generating functions and complex analysis were discovered by Legendre, Abel, and Jacobi (1820s). This was a bit of an accident: they were trying to understand the integrals that come up when trying to compute arclengths on an ellipse.[4]

This theory was further developed by Weierstrass (1860s). One key example is the *discriminant modular form*

$$\Delta(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24},$$

which has a strong symmetry property: for $q = e^{2\pi i \tau}$ with $\mathrm{Im}(\tau) > 0$ and $a, b, c, d \in \mathbb{Z}$ with $ad - bc = 1$,

$$\Delta\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{12} \Delta(\tau)$$

[4] These are closely related to *elliptic curves*, whence that terminology.

Analytic properties of generating functions

Some deep links between combinatorial generating functions and complex analysis were discovered by Legendre, Abel, and Jacobi (1820s). This was a bit of an accident: they were trying to understand the integrals that come up when trying to compute arclengths on an ellipse.[4]

This theory was further developed by Weierstrass (1860s). One key example is the *discriminant modular form*

$$\Delta(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24},$$

which has a strong symmetry property: for $q = e^{2\pi i \tau}$ with $\mathrm{Im}(\tau) > 0$ and $a, b, c, d \in \mathbb{Z}$ with $ad - bc = 1$,

$$\Delta\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{12} \Delta(\tau)$$

[4] These are closely related to *elliptic curves*, whence that terminology.

An amazing observation

Let's look at some coefficients of Δ:

$$\begin{aligned}\Delta(q) = q &- 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 \\ &+ 84480q^8 - 113643q^9 - 115920q^{10} + 534612q^{11} - 370944q^{12} \\ &- 577738q^{13} + 401856q^{14} + 1217160q^{15} + 987136q^{16} - \cdots\end{aligned}$$

Write $\tau(n)$ for the coefficient of q^n. Ramanujan (1916) observed:

$$\tau(mn) = \tau(m)\tau(n) \qquad \text{whenever } \gcd(m,n) = 1.$$

This was explained by Mordell (1917) and generalized by Hecke (1937).

For more about Δ, see its "home page" (more on which shortly):

`http://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/1/12/1/a/`.

An amazing observation

Let's look at some coefficients of Δ:

$$\begin{aligned}\Delta(q) = q &- 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 \\ &+ 84480q^8 - 113643q^9 - 115920q^{10} + 534612q^{11} - 370944q^{12} \\ &- 577738q^{13} + 401856q^{14} + 1217160q^{15} + 987136q^{16} - \cdots\end{aligned}$$

Write $\tau(n)$ for the coefficient of q^n. Ramanujan (1916) observed:

$$\tau(mn) = \tau(m)\tau(n) \qquad \text{whenever } \gcd(m,n) = 1.$$

This was explained by Mordell (1917) and generalized by Hecke (1937).

For more about Δ, see its "home page" (more on which shortly):

`http://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/1/12/1/a/`.

An amazing observation

Let's look at some coefficients of Δ:

$$\begin{aligned}\Delta(q) = q &- 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 \\ &+ 84480q^8 - 113643q^9 - 115920q^{10} + 534612q^{11} - 370944q^{12} \\ &- 577738q^{13} + 401856q^{14} + 1217160q^{15} + 987136q^{16} - \cdots\end{aligned}$$

Write $\tau(n)$ for the coefficient of q^n. Ramanujan (1916) observed:

$$\tau(mn) = \tau(m)\tau(n) \qquad \text{whenever } \gcd(m,n) = 1.$$

This was explained by Mordell (1917) and generalized by Hecke (1937).

For more about Δ, see its "home page" (more on which shortly):

`http://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/1/12/1/a/`.

An amazing observation

Let's look at some coefficients of Δ:

$$\begin{aligned}\Delta(q) = q &- 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 \\ &+ 84480q^8 - 113643q^9 - 115920q^{10} + 534612q^{11} - 370944q^{12} \\ &- 577738q^{13} + 401856q^{14} + 1217160q^{15} + 987136q^{16} - \cdots\end{aligned}$$

Write $\tau(n)$ for the coefficient of q^n. Ramanujan (1916) observed:

$$\tau(mn) = \tau(m)\tau(n) \qquad \text{whenever } \gcd(m,n) = 1.$$

This was explained by Mordell (1917) and generalized by Hecke (1937).

For more about Δ, see its "home page" (more on which shortly):

`http://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/1/12/1/a/`.

A related example

A closely related example is the modular form

$$f(q) = q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2.$$

It again has a transformation rule: for $q = e^{2\pi i \tau}$,

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 f(\tau) \quad (a, b, c, d \in \mathbb{Z}, ad - bc = 1, 11|c).$$

Writing a_n for the coefficient of q^n in f, one again has multiplicativity:

$$a_{mn} = a_m a_n \qquad (\gcd(m, n) = 1).$$

Like Δ, f is found in the *L-Functions and Modular Forms Database*:

`http://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/11/2/1/a/`.

A related example

A closely related example is the modular form

$$f(q) = q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2.$$

It again has a transformation rule: for $q = e^{2\pi i \tau}$,

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 f(\tau) \quad (a, b, c, d \in \mathbb{Z}, ad - bc = 1, 11|c).$$

Writing a_n for the coefficient of q^n in f, one again has multiplicativity:

$$a_{mn} = a_m a_n \qquad (\gcd(m, n) = 1).$$

Like Δ, f is found in the *L-Functions and Modular Forms Database*:

`http://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/11/2/1/a/`.

A related example

A closely related example is the modular form

$$f(q) = q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2.$$

It again has a transformation rule: for $q = e^{2\pi i \tau}$,

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 f(\tau) \quad (a, b, c, d \in \mathbb{Z}, ad - bc = 1, 11|c).$$

Writing a_n for the coefficient of q^n in f, one again has multiplicativity:

$$a_{mn} = a_m a_n \qquad (\gcd(m, n) = 1).$$

Like Δ, f is found in the *L-Functions and Modular Forms Database*:

`http://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/11/2/1/a/`.

A related example

A closely related example is the modular form

$$f(q) = q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2.$$

It again has a transformation rule: for $q = e^{2\pi i \tau}$,

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 f(\tau) \quad (a, b, c, d \in \mathbb{Z}, ad - bc = 1, 11|c).$$

Writing a_n for the coefficient of q^n in f, one again has multiplicativity:

$$a_{mn} = a_m a_n \qquad (\gcd(m, n) = 1).$$

Like Δ, f is found in the *L-Functions and Modular Forms Database*:

`http://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/11/2/1/a/`.

From a modular form to an elliptic curve

Starting from the modular form

$$f(q) = q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2,$$

a construction of Eichler and Shimura (1950s) produces the elliptic curve

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

It also has a home page: `http://www.lmfdb.org/EllipticCurve/Q/11/a/2`.

These two objects have the following relationship: for $p \neq 11$ a prime, there are exactly $p - a_p$ pairs $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ satisfying the equation of the elliptic curve, where again a_p is the coefficient of q^p in f.

Many numerical examples of this sort have been tabulated by Cremona (1990s–present; see `http://lmfdb.org`). By the work of Wiles (and followup), it is known that *every* elliptic curve over $\mathbb{Q}$ arises in this fashion.

From a modular form to an elliptic curve

Starting from the modular form

$$f(q) = q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2,$$

a construction of Eichler and Shimura (1950s) produces the elliptic curve

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

It also has a home page: `http://www.lmfdb.org/EllipticCurve/Q/11/a/2`.

These two objects have the following relationship: for $p \neq 11$ a prime, there are exactly $p - a_p$ pairs $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ satisfying the equation of the elliptic curve, where again a_p is the coefficient of q^p in f.

Many numerical examples of this sort have been tabulated by Cremona (1990s–present; see `http://lmfdb.org`). By the work of Wiles (and followup), it is known that *every* elliptic curve over $\mathbb{Q}$ arises in this fashion.

From a modular form to an elliptic curve

Starting from the modular form

$$f(q) = q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2,$$

a construction of Eichler and Shimura (1950s) produces the elliptic curve

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

It also has a home page: `http://www.lmfdb.org/EllipticCurve/Q/11/a/2`.

These two objects have the following relationship: for $p \neq 11$ a prime, there are exactly $p - a_p$ pairs $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ satisfying the equation of the elliptic curve, where again a_p is the coefficient of q^p in f.

Many numerical examples of this sort have been tabulated by Cremona (1990s–present; see `http://lmfdb.org`). By the work of Wiles (and followup), it is known that *every* elliptic curve over $\mathbb{Q}$ arises in this fashion.

From a modular form to an elliptic curve

Starting from the modular form

$$f(q) = q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2,$$

a construction of Eichler and Shimura (1950s) produces the elliptic curve

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

It also has a home page: `http://www.lmfdb.org/EllipticCurve/Q/11/a/2`.

These two objects have the following relationship: for $p \neq 11$ a prime, there are exactly $p - a_p$ pairs $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ satisfying the equation of the elliptic curve, where again a_p is the coefficient of q^p in f.

Many numerical examples of this sort have been tabulated by Cremona (1990s–present; see `http://lmfdb.org`). By the work of Wiles (and followup), it is known that *every* elliptic curve over $\mathbb{Q}$ arises in this fashion.

More analytic functions

There is a close relationship between an analytic function of τ of the form

$$\sum_{n=1}^{\infty} a_n q^n \qquad (q = e^{2\pi i \tau})$$

and the corresponding function of s given by the *Dirichlet series*

$$\sum_{n=1}^{\infty} a_n n^{-s}.$$

Information about the latter can be used to understand the aggregate (statistical) behavior of the a_n as n varies. For example, if $a_n = 1$ for all n, then the Dirichlet series is the *Riemann zeta function*, which can be used to prove the *prime number theorem*.

More analytic functions

There is a close relationship between an analytic function of τ of the form

$$\sum_{n=1}^{\infty} a_n q^n \qquad (q = e^{2\pi i \tau})$$

and the corresponding function of s given by the *Dirichlet series*

$$\sum_{n=1}^{\infty} a_n n^{-s}.$$

Information about the latter can be used to understand the aggregate (statistical) behavior of the a_n as n varies. For example, if $a_n = 1$ for all n, then the Dirichlet series is the *Riemann zeta function*, which can be used to prove the *prime number theorem*.

Dirichlet series and elliptic curves

Recall that if a modular form $f = \sum_{n=1}^{\infty} a_n q^n$ and an elliptic curve E are related as per Eichler-Shimura, then for p prime (with finitely many exceptions), the number of points on E over $\mathbb{F}_p$ equals $p + 1 - a_p$.

It was shown[5] by Hasse (1930s) that $|a_p| \leq 2\sqrt{p}$. So one might ask how $a_p/\sqrt{p}$ varies in the interval $[-2, 2]$ as p varies.

A conjecture of Sato and Tate (1960s) asserts that there are only two possible answers, depending on whether E has *complex multiplication*. This is now known by work of Taylor et al (2000s), amounting to progress on the vast *Langlands program* (building on Wiles).

For illustrations, see:

`http://math.mit.edu/~drew/g1_D1_a1f.gif`
`http://math.mit.edu/~drew/g1_D2_a1f.gif`

[5] Ramanujan conjectured a similar statement about Δ, whose resolution requires the full strength of Deligne's proof of the *Weil conjectures* (1970s).

Dirichlet series and elliptic curves

Recall that if a modular form $f = \sum_{n=1}^{\infty} a_n q^n$ and an elliptic curve E are related as per Eichler-Shimura, then for p prime (with finitely many exceptions), the number of points on E over $\mathbb{F}_p$ equals $p + 1 - a_p$.

It was shown[5] by Hasse (1930s) that $|a_p| \leq 2\sqrt{p}$. So one might ask how $a_p/\sqrt{p}$ varies in the interval $[-2, 2]$ as p varies.

A conjecture of Sato and Tate (1960s) asserts that there are only two possible answers, depending on whether E has *complex multiplication*. This is now known by work of Taylor et al (2000s), amounting to progress on the vast *Langlands program* (building on Wiles).

For illustrations, see:

`http://math.mit.edu/~drew/g1_D1_a1f.gif`
`http://math.mit.edu/~drew/g1_D2_a1f.gif`

[5] Ramanujan conjectured a similar statement about Δ, whose resolution requires the full strength of Deligne's proof of the *Weil conjectures* (1970s).

Dirichlet series and elliptic curves

Recall that if a modular form $f = \sum_{n=1}^{\infty} a_n q^n$ and an elliptic curve E are related as per Eichler-Shimura, then for p prime (with finitely many exceptions), the number of points on E over $\mathbb{F}_p$ equals $p + 1 - a_p$.

It was shown[5] by Hasse (1930s) that $|a_p| \leq 2\sqrt{p}$. So one might ask how $a_p/\sqrt{p}$ varies in the interval $[-2, 2]$ as p varies.

A conjecture of Sato and Tate (1960s) asserts that there are only two possible answers, depending on whether E has *complex multiplication*. This is now known by work of Taylor et al (2000s), amounting to progress on the vast *Langlands program* (building on Wiles).

For illustrations, see:

`http://math.mit.edu/~drew/g1_D1_a1f.gif`
`http://math.mit.edu/~drew/g1_D2_a1f.gif`

[5] Ramanujan conjectured a similar statement about Δ, whose resolution requires the full strength of Deligne's proof of the *Weil conjectures* (1970s).

Dirichlet series and elliptic curves

Recall that if a modular form $f = \sum_{n=1}^{\infty} a_n q^n$ and an elliptic curve E are related as per Eichler-Shimura, then for p prime (with finitely many exceptions), the number of points on E over $\mathbb{F}_p$ equals $p + 1 - a_p$.

It was shown[5] by Hasse (1930s) that $|a_p| \leq 2\sqrt{p}$. So one might ask how $a_p/\sqrt{p}$ varies in the interval $[-2, 2]$ as p varies.

A conjecture of Sato and Tate (1960s) asserts that there are only two possible answers, depending on whether E has *complex multiplication*. This is now known by work of Taylor et al (2000s), amounting to progress on the vast *Langlands program* (building on Wiles).

For illustrations, see:

`http://math.mit.edu/~drew/g1_D1_a1f.gif`
`http://math.mit.edu/~drew/g1_D2_a1f.gif`

[5] Ramanujan conjectured a similar statement about Δ, whose resolution requires the full strength of Deligne's proof of the *Weil conjectures* (1970s).

I could go on, but...

I'll stop here. thank you for your attention!