Arithmetic and some of its aspirations: notes for my talk to the *Friends of the Harvard Mathematics Department*; May 5, 2009

Barry Mazur

May 18, 2009

I was invited by our chairman to talk broadly about Number Theory this morning—to give something of an overview. What a delightful thing to do.

For this mission there is no better starting place than with something that is both intensely specific, and strangely unifying—say, Felix Klein's **elliptic modular function**. The elliptic modular function, usually denoted $j(z)$, is analytic on the upper half of the complex plane

$$z \;=\; x + iy, \qquad y > 0$$

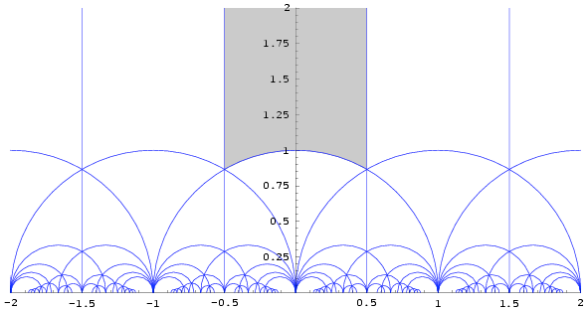
and has a famous Fourier expansion:

$$j(z) \;=\; e^{-2\pi iz} + 744 + 196884e^{2\pi iz} + 21493760e^{4\pi iz} + 864299970e^{6\pi iz} + 20245856256e^{8\pi iz} + \cdots$$

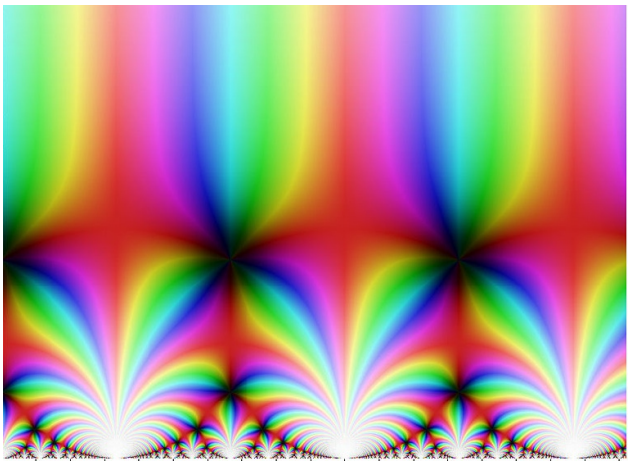
all coefficients being positive integers. The elliptic modular function

- is loved by *the complex analysts* since it is invariant the hidden symmetry $z \mapsto -1/z$, and the value $j(z)$ for any complex number z determines the orbit of z under the action of linear fractional transformations
$$z \mapsto \frac{az+b}{cz+d}$$
for matrices
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}).$$

- is loved by *the hyperbolic geometers* since, thanks to this symmetry, it tiles the hyperbolic plane:



Nowadays there are various ways of revealing this tiling by choosing a color spectrum for the argument of the complex values of the function $j(z)$:



- The function $j(z)$ is loved by *the finite group theorists* since the coefficients

$$196884, \quad 21493760, \quad 864299970, \quad 20245856256, \cdots$$

are the dimensions of a famous series of linear representations of the simple group known as the *Monster*—a rather big finite group, of order

$$808017424794512875886459904961710757005754368000000000,$$

its smallest nontrivial linear representation being of the whopping dimension 196883.

It was John McKay who noticed that the first interesting Fourier coefficient 196884 of the elliptic modular function satisfies the equation:

$$196884 \quad = \quad 196883 \; + \; 1$$

and therefore is the dimension of a (faithful) representation representation of the Monster group. This simple "equation" observed by McKay set off an amazing cascade of discoveries.

- It was loved by *Klein* himself since he showed that his elliptic modular function provides the vocabulary in which to give explicit solutions of the general quintic polynomial—whose roots could *not* be expressed in terms of radicals such as the 16c Italian mathematicians used to solve third and fourth degree polynomials;

- and it is loved by the followers of *Ramanujan* who find a world of structure in the congruence properties of the Fourier coefficients;

  E.g.: For every n

  - the $2n$-th Fourier coefficient of $j(z)$ is even,
  - the $3n$-th Fourier coefficient of $j(z)$ is divisible by 3,
  - the $5n$-th Fourier coefficient of $j(z)$ is divisible by 5,
  - the $7n$-th Fourier coefficient of $j(z)$ is divisible by 7,
  - the $11n$-th Fourier coefficient of $j(z)$ is divisible by 11,

  but this pattern breaks down for $p = 13$.

- The elliptic modular function is loved by the analysts, arithmeticians and algebraic geometers who study elliptic curves since the isomorphism class of the elliptic curve formed by the lattice generated by the complex numbers 1 and z is completely determined by $j(z)$, usually referred to as the *j-invariant* of the elliptic curve. It is the showcase example of a *modulus* in algebraic geometry, i.e., a continuous parameter that classifies a continuously varying array of distinct isomorphism classes of mathematical objects.

$\{$ *The isomorphism class of the elliptic curve E formed by the lattice generated by* 1 *and* $z\}$

$$\updownarrow$$

$\{$ *The complex number $j(z)$, usually referred to as the j-invariant of the elliptic curve E*$\}$.

- AND it was loved by Leopold Kronecker who hitched the aspirations of his youth (his *Jugendtraum*) on the ability of the elliptic modular function to help generate, in a magically ordered way, all algebraic numbers that are relatively abelian over quadratic imaginary number fields.

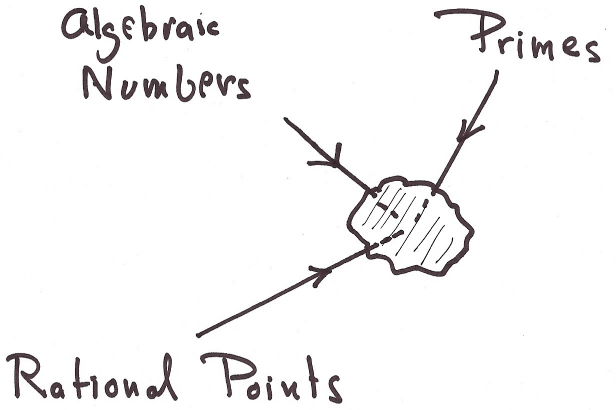
So, lots of love has been showered on this elliptic modular function $j(z)$—it shows up in various mathematical disciplines performing its miracles in each—but even now, I think, we still don't know in a fully satisfying sense what *it* is, or what deep structure it is offering us glimmers of, and how it comes to play its unifying role.

In this hour I want to push off in the Kronecker direction, explain a tiny bit of Kronecker's specific ambition, But I also want to interpret "Kronecker's dream" much more loosely than he himself would be comfortable with (i.e., I am taking the usual prerogative of *interpreters of dreams*)! It is reasonable to view the Jugendtraum as blending into a very modern ambition: the on-going attempt to come to grips with what number theorists and algebraic geometers call *the theory of motives*.

Before getting to this, I should offer a disclaimer, for we will not be seeing anything like an overview of the broad span of modern arithmetic research. Think of Arithmetic as some form of Geology where the *basic subject* is a mass of a certain shape, and where the surface features are somewhat accessible to any of us, if we travel a bit around it[1] but the real reasons why it[2] is what it is—and even *what* it is—is hidden within its interior. The real secret of its unity lies, perhaps, in its center.

[1] E.g., there are prime numbers comprising the building blocks of multiplication of whole numbers, and there are infinitely many of these, etc.

[2] I.e., the *it* is *the earth,* for Geology; and *the structure of Number* for Arithmetic.



What can we do to study it? We can drill here and there to sample its composition and to understand a tiny bit better the forces that hold it together. Where we start to drill depends on accidents: our own location, our predisposition, and what things occur to us. But the ultimate aim is to understand the center.

Here are a few traditional drilling sites:

1. Numbers defined by algebraic formulas, and the structure of interesting aggregates of these numbers.
2. Interesting arithmetic phenomena and the delicate statistical data that they generate.
3. Algorithmically generated lists of numbers, as described in the vocabulary of polynomial equations.

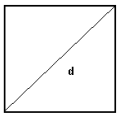
There are many other ways than these to study Arithmetic but I mention these three aspects of our subject for they are intimately related to disparate fields of mathematics. For example, going down the above lists we have these related disciplines involved:

1. Algebraic geometry, Algebraic topology, representation theory of algebraic groups
2. Complex analysis, Fourier analysis
3. Mathematical logic

I've chosen to focus, this morning, on the first of these topics:

1 Numbers defined by algebraic formulas, and how to organize aggregates of these numbers.

The ratio $\frac{diagonal}{side}$ of a square was, in antiquity an example of a proportion that could not be expressed as a ratio of whole numbers—and therefore unapproachable by standard means,



And yet this diagonal has the comforting property that if you built a second square with side equal to it (i.e. to the diagonal of the square in Diagram 1) the ratio of the areas of the two squares is easy to understand (i.e., it is 2).

Put in modern algebraic terms, we have that $\sqrt{2}$ is irrational, and nevertheless can be pinpointed by the fact that it is a (positive) root of the simple polynomial $X^2 - 2$. Of course, the ancients had quite few other such successes, such as the understanding of the ratio $\sqrt{5}$ and its involvement with the construction of the regular pentagon. They also had their nonsuccesses (and bewilderment) as in the issue of duplication of the cube, trisection of a general angle, and even worse: the squaring of the circle.

The general concept emerging[3] is that of *algebraicity* versus *transcendence*.

Definition 1 *An* **algebraic number** θ *is one that is a root of a polynomial with rational coefficients. In other words, a number is* **algebraic** *if it satisfies a polynomial relation (with rational coefficients).*

The simplest of these would be those expressed by radicals, and in fact, the ones expressed by radical were the ones most immediately encountered in geometry, or as roots of low degree polynomials. For example "Cardan's Formula" tells us that the roots of the general cubic polynomial $X^3 + aX + b$ (the coefficients a, b can be any sort of number) are given by

$$\sqrt[3]{\frac{1}{2}(-c + \sqrt{c^2 + \frac{4a^3}{27}})} + \sqrt[3]{\frac{1}{2}(-c - \sqrt{c^2 + \frac{4a^3}{27}})}.$$

The utility of numbers defined by algebraic relations needs no advertisement. The issue is rather that algebraic numbers are so ubiquitous and there are *so many of them*—see Book X of Euclid which is a big big mess!—that one is in great need of effective strategies with which to study classes of them systematically. Sometimes algebraic numbers show up in neatly organized arrays:

[3]The much-used word *emergence* which puts in the shadows the people who work on concepts and gives agency to the concepts themselves as they"emerge into the light" isn't—I think—a cop-out word here, given the slow maturation of the concepts of algebraicity, and transcendence.

2 Roots of unity as a cluster of supremely organized algebraic numbers

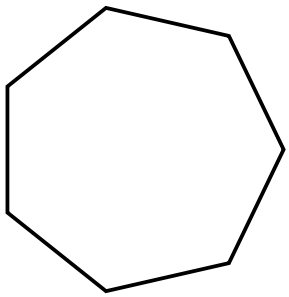
At the end of the eighteenth century, and beginning of the nineteenth century it was understood (largely by Gauss, I think) that the construction of the regular n-gon was strictly related to the understanding of the algebraic numbers that are now called *roots of unity*. That is, the vertices of the regular n-gon centered at the origin and inscribed in the circle of radius 1 are the complex number of the form

$$e^{\frac{2\pi ia}{n}}$$

and these are precisely the roots of the polynomial

$$X^n - 1.$$

In particular, roots of unity are algebraic numbers.



For example, the vertices of the above heptagon are complex algebraic numbers that are roots of the polynomial $X^7 - 1$. Another way of thinking of this structure is to consider the heptagon as a *machine whose symmetries "generate" the algebraic numbers*

$$e^{2\pi i/7}, e^{4\pi i/7}, e^{6\pi i/7}, e^{8\pi i/7}, e^{10\pi i/7}, e^{12\pi i/7}$$

Roots of unity are examples of what one might call **abelian algebraic numbers over the rational field Q** which comprise a largish class of algebraic numbers that are—from a certain perspective—easier to deal with than the general algebraic number. Their definition is elementary and natural if one is happy with Galois theory; I'll give it in this footnote[4].

It was about that time (beginning of the nineteenth century that the focus on *aggregates* of algebraic numbers took off; that is, on the structure of rings and fields of algebraic numbers (rather than on algebraic numbers, one at a time, each in isolation). Galois theory emerged as a way of organizing this data in a computationally and conceptually powerful way.

Roots of unity, for a while, formed the main crucial repertoire of interesting algebraic numbers whose arithmetic could be somewhat—even though hardly perfectly—understood.

3 The Kronecker-Weber Theorem

Kronecker and Weber, at the end of the nineteenth century, proved the following surprising and powerful mind-focusing result:

> Any abelian algebraic number can be expressed as a finite linear combination (with rational numbers as coefficients) of roots of unity, or equivalently: of the *values of the transcendental function* $e^{2\pi iz}$ *as* z *runs through a collection of rational numbers*[5].

[4]Define an **abelian algebraic number over Q** to be one that is

- the root of a polynomial with rational coefficients (i.e., is *algebraic*) and such that
- any two permutations A, B of the roots of that polynomial that *preserve all polynomial relations (with rational coefficients) among the roots*, are permutations that commute; i.e., $A \cdot B = B \cdot A$.

For example, any quadratic irrationality such as $\sqrt{d}$ for d a nonsquare integer *is* abelian since the irreducible polynomial over the rationals that has it as a root, has *only* two roots (it and one other) and any two permutations of those meager two roots commute. But, say, $\sqrt[m]{2}$ are nonabelian algebraic numbers if $m > 2$.

As with most algebraic notions, Galois theory gave us the vocabulary to define analogues of these notions *relative to a given field* replacing the rational field **Q** with an arbitrary field. So too here. One defines the concept of **abelian algebraic number over a field** K to be as above, but with the rational field replaced systematically in the definition by the field K.

[5]For example, since quadratic irrationalities are abelian algebraic numbers they are linear combos of roots of unity: indeed they are by a prior celebrated theorem of Gauss that gives a completely explicit formula for this; for example:

$$\pm i^{\frac{p-1}{2}}\sqrt{p} = e^{2\pi i/p} + \binom{2}{p}e^{4\pi i/p} + \binom{3}{p}e^{6\pi i/p} + \ldots + \binom{-2}{p}e^{-4\pi i/p} + \binom{-1}{p}e^{-2\pi i/p},$$

where the coefficients in this linear combination are ± 1 and more specifically: $\binom{a}{p}$ is $+1$ if a is a *quadratic residue modulo* p; that is, if a is congruent to the square of an integer modulo p and -1 if not; and even the ambiguous $\pm$ in the formula can be pinned down in a closed form. By the way: if you considered a cubic polynomial $X^3 + bX + c$ with $b, c, \in \mathbf{Q}$ of square discriminant, its roots would again be linear combos (with rational coefficients) of roots of unity but *I don't know of any general explicit expression for such linear combos, as we have for quadratic algebraic numbers via the Gauss sum formulation.*

To gauge how mathematicians, on occasion, expressed exuberance over this, count the "wunderbars" in the following (word-for-word) transcription of a piece of a lecture David Hilbert gave in his course (*Vorlesung über die Theorie der Algebraischen Zahlen*) in 1926[6].

> Das ist etwas ganz Eigenartiges. Wir besitzen eine analytische Funktion $e^{2\pi iz}$ mit der wunderbaren Eigenschaft, dass sie für rationale Argumentwert immer algebraische Werte liefert und dass man durch sie alle Abelschen Körper und nur diese erhält. Diese zweite Eigenschaft ist ja der Inhalt des grossen Kroneckerschen Satzes, dass alle Abelschen Körper Kreiskörper sind. Dass ist nun in der Tat eine ganz wunderbare Eigenschaft. Schon allein dass eine transzendente Function algebraiche Werte liefert, wenn man das Argument $z = a/b$ setzt! Dass es so etwas überhaupt gibt! Das Seltsame ist nun dabei, dass man nur die Funktion $e^{2\pi iz}$ zu besitzen braucht und dass dann alles andere sich ganz von selbst, förmlich ohne unser Hinsutun sich einstellt! Dass gilt also für das Problem, alle Abelschen Körper über den Körper der rationalen Zahlen aufzustellen. Unser neues Problem heisst nun, alle Abelschen Körper über dem imaginär quadratischen Körper $k(\sqrt{m})$ $m < 0$ zu erhalten. Für die Erledigung des ersten Problems stellte such uns de Funktion $e^{2\pi iz}$ zur Verfügung, dieser wunderbare Geschenk des Himmels. Werden wir nun auch für den zweiten Fall etwas Aehnliches erhalten? Das ist de Frage, die wir auch gar nicht umgehen können.

But what economy! And what a template! Any abelian algebraic number over $\mathbf{Q}$ is a linear combination of roots of unity, with rational coefficients. We can think of the exponential function as a homomorphism of groups

$$\mathbf{C} \longrightarrow \mathbf{C}^*$$

where $\mathbf{C}$ is the complex plane viewed as group under addition and $\mathbf{C}^*$ the complex plane with the origin removed, viewed as group under multiplication. The roots of unity, then, are just the points of finite order in the multiplicative group $\mathbf{C}^*$.

Let us think of this structure—the exponential function

$$z \quad \mapsto \quad e^{2\pi iz}$$

viewed as homomorphism $\mathbf{C} \to \mathbf{C}^*$—as a **unifier**. For this *single function* generates in a systematic and coherent way *all* abelian algebraic numbers, as its values for rational arguments z.

Are there other "unifiers" in the broader context of algebraic number theory? Hilbert, in the quotation above, is preparing us for this with his

> Unser neues Problem heisst nun, alle Abelschen Körper über dem imaginär quadratischen Körper $k(\sqrt{m})$ $m < 0$ zu erhalten.

That is, given any quadratic imaginary number field

$$\mathbf{Q}(\sqrt{-1}), \text{ or } \mathbf{Q}(\sqrt{-2}), \text{ or } \mathbf{Q}(\sqrt{-3}), \text{ or } \ldots$$

[6]I'm thankful to Yuri Tschinkel and the Göttingen library for permission to quote from these notes.

is there a *unifier* that organizes as fully and in as revealing a way, all the abelian algebraic numbers over that field, just as the exponential function does for the field of rational numbers $\mathbf{Q}$?

4 Kronecker's Dream

Kronecker saw that if you add to the exponential function, merely *one* further function (*Klein's elliptic modular function*) you had the key to unification of all the abelian algebraic numbers of all these fields. Exactly as with exponential function, where you formed the values $e^{2\pi iz}$ for z rational numbers, you were requested by Kronecker to consider the values $j(z)$ for z ranging through your quadratic imaginary field, and

- these numbers are *algebraic numbers*—this being already a miracle and is by no means evident from the power series formulation in any instance; for example

  $$j(\frac{1+\sqrt{-23}}{2})$$

  turns out to be a root of the polynomial

  $$X^3 + 3491750X^2 - 5151296875X + 12771880859375.$$

- The values $j(z)$ for z ranging through your quadratic imaginary field are abelian algebraic numbers over the field—another miracle— for example the Galois group of the polynomial $X^3 + 3491750X^2 - 5151296875X + 12771880859375$ is abelian (cyclic of order three) over $\mathbf{Q}(\sqrt{-23})$ and,

- The values $j(z)$ for z ranging through your quadratic imaginary field together with roots of unity, will essentially generate *all* abelian algebraic numbers over the field.

Again: what a template, and what a unification!

5 Nonabelian dreams: first encounter

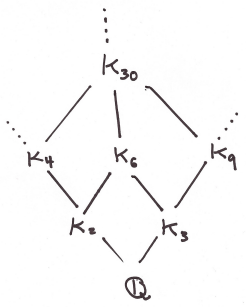
You might think—and you'd be right—that the essential unifying power of the exponential function, and its ability to organize, for us, all abelian algebraic numbers of $\mathbf{Q}$ comes from the mere fact that there is an underlying (large, continuous) algebraic group, namely the multiplicative group $\mathbf{C}^*$, and we are systematically generating algebraic numbers by considering the elements of finite order in that large group. The group, then is the unifying principle. If you have another algebraic group E over a number field (elliptic curves have been very successfully used for this type of work; more generally commutative groups turn out to be best for this) its points of finite order will have coordinates that are algebraic numbers, and the splay of algebraic numbers that you get will be—often—supremely organized by the *unifier*: the algebraic group E from which they sprang. From

this perspective, the theory of (commutative) algebraic groups over number fields becomes a huge factory for the production of beautifully organized constellations of algebraic numbers.

An example of this is the elliptic curve

$$E: \qquad y^2 + y \;=\; x^3 - x.$$

For every positive integer N, the points of order N have coordinates that generate a field extension of $\mathbf{Q}$ that is Galois with Galois group $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ and this infinite family of field extensions K_N of increasing degree are—in a very concrete sense—all tied together by the unifying principle of this elliptic curve. We have here a treasure-chest of usable algebraic numbers generating this array of number fields.



I doubt that there is a contemporary number theorist who works with this structure who isn't continuously amazed by the efficacy of this unifying method for the study of otherwise unapproachable arrays of algebraic numbers—just as Hilbert was amazed by the organizing power of the exponential function. But ... as I mentioned above, there are indeed lots of algebraic numbers and we are in serious need of more powerful unifying structures to deal with them.

6 Nonabelian dreams: second encounter (the theory of motives)

So far, we have talked about these organizing principles for the study of algebraic numbers en masse:

- The exponential function $e^{2\pi iz}$,
- The extraction of radicals more generally,
- the elliptic modular function $j(z)$,
- Elliptic curves, and (commutative) algebraic groups more generally.

A current version of Kronecker's dream is to extend this already impressive list, and to deputize all of algebraic geometry over number fields to serve as vast "unifiers" of constellations of algebraic numbers.

For this one turns to the still-in-progress *theory of motives* initiated by Grothendieck. Grothendieck[7] envisioned associating to V, any object of algebraic geometry (any *algebraic variety*, i.e., a space defined by algebraic equations) a *simpler object* that I'll just call $H(V)$ and we can refer to it as **the motive of** V. Think of this "simpler object" $H(V)$ as having a linear structure like a vector space.

Moving, then, from V to $H(V)$ loses lots of information contained in the objects of Algebraic Geometry but, in contrast, it retains—in perhaps especially usable form—some important structure:

$$\{\text{ALGEBRAIC GEOMETRY}\} \longrightarrow \{\text{THEORY OF MOTIVES}\}$$

$$V \mapsto H(V).$$

This passage might be thought of as a modern move akin to *The Calculus* (which linearizes—at an infinitesimal level— nonlinear functions). For, thinking of $H(V)$ as—say—a vector space, i.e., linear, and thinking of the original V as some—possibly nonlinear—space defined by polynomial equations, we have gained simplification, even if we have lost detailed structure via this passage.

The main feature of this passage is that it is natural, and is very helpful in understanding symmetries; in particular any symmetry of V gives rise to a corresponding linear symmetry of $H(V)$.

$$\{\text{Symmetries of } V\}$$
$$\downarrow$$
$$\{\text{Symmetries of } H(V)\}$$

The space V is a machine whose symmetries acting linearly on $H(V)$ "generate" a vast number of algebraic numbers in a coherent way.

[7] Here is Grothendieck reflecting on the synthesis of various cohomology theories that comprises part of his vision:

" Contrary to what occurs in ordinary topology, one finds oneself confronting a disconcerting abundance of different cohomological theories. One has the distinct impression (but in a sense that remains vague) that each of these theories "amount to the same thing," that they "give the same results." In order to express this intuition, of the kinship of these different cohomological theories, I formulated the notion of "motive" associated to an algebraic variety. By this term, I want to suggest that it is the "common motive" (or "common reason") behind this multitude of cohomological invariants attached to an algebraic variety, or indeed, behind all cohomological invariants that are a priori possible."

To summarize: if V is defined by polynomial equations over a number field K then, $H(V)$ will be naturally endowed with a linear action of the Galois group of the algebraic closure of K thereby generating a (usually vast) constellation of algebraic numbers over K, as supremely organized as the other arrays of algebraic numbers we have talked about in previous sections.

In this way, *every* algebraic variety V over a number field becomes a formidable unifier[8] for algebraic number theory.

To mine all this to the fullest is one of our current dreams!

[8]Perhaps the most well known such "unifier" that is not of the sort discussed in the previous section is a certain 12-dimensional algebraic variety $\mathcal{V}$ that has the property that a piece of its $H(\mathcal{V})$ provides us with a large array of algebraic number fields whose arithmetic can be understood in depth if we just know the Ramanujaun tau-function

$$n \mapsto \tau(n),$$

i.e., the coefficients of the power series

$$\Delta \;=\; q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n+1}^{\infty}\tau(n)q^n.$$