Ramanujan's Tau Function

With a Focus on Congruences

8 May 2007

Abstract

We will be concerned with Ramanujan's τ function defined by

$$\Delta \triangleq q\,\theta(q)^{24} \triangleq q\prod_{n\geqslant 1}(1-q^n)^{24} = \sum_{n\geqslant 1}\tau(n)\,q^n.$$

The Ramanujan numbers $\tau(n)$ appear as sequence `A000594` in [Sloane, 2007]. Their first few values are

$$1, -24, 252, -1472, 4830, -6048, -16744, 84480, -113643.$$

We'll have a special interest in congruences for $\tau(n)$. One of the historical motivations for such congruences has been the hope to establish Lehmer's conjecture, namely that $\tau(n)\neq 0$ for all n, based on congruence considerations.

On our way, we will have to make use of some machinery involving modular forms. The basic theory we need will be briefly sketched.

Contents

Armin Straub
math@arminstraub.com

1 A First Class of Simple Congruences

Our first class of congruences which are due to Ramanujan, see [Berndt and Ono, 1999], will stem from the following simple observation.

Lemma 1. *For any prime p,*

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

This gives us for example,

$$q\prod_{n\geqslant 1}(1-q^n)^{24} \equiv q\prod_{n\geqslant 1}(1-q^n)^3\prod_{n\geqslant 1}(1-q^{7n})^3 \pmod{7}.$$

In more compact form this reads as

$$q\,\theta(q)^{24} \equiv q\,\theta(q)^3\,\theta(q^7)^3 \pmod{7}.$$

We'll now examine the right-hand side more closely to find congruences of the type

$$\tau(7n+\alpha)\equiv 0 \pmod{7}.$$

To establish such a result we check if the coefficient of $q^{7n+\alpha}$ in $q\,\theta(q)^3$ is a multiple of 7. The same line of reasoning works for any prime less than 24 but the details and final results vary a lot.

Modulus 7. As mentioned before we have

$$q\,\theta(q)^{24} \equiv q\,\theta(q)^3\,\theta(q^7)^3 \pmod{7},$$

and we are interested in the coefficient of $q^{7n+\alpha}$ in $q\,\theta(q)^3$. To this end, note that by Jacobi's identity

$$q\,\theta(q)^3 = q\sum_{n\geqslant 0}(-1)^n(2n+1)\,q^{n(n+1)/2}.$$

So the only exponents appearing here are of the form

$$\frac{n(n+1)}{2}+1 \equiv 0,1,2,4 \pmod{7}.$$

Further, $2n+1$ is a multiple of 7 if $n\equiv 3$ in which case the exponent is of the form $7n$. Thus,

$$\tau(7n),\ \tau(7n+3),\ \tau(7n+5),\ \tau(7n+6)\equiv 0 \pmod{7}.$$

$3,5,6$ are the quadratic non-residues.

Modulus 23. Here

$$q\,\theta(q)^{24} \equiv q\,\theta(q)\,\theta(q^{23}) \pmod{23},$$

and we make use of the pentagonal number theorem

$$q\,\theta(q) = q\sum_{n}(-1)^n\,q^{n(3n+1)/2}.$$

The exponents are of the form

$$\frac{n\,(3n\pm 1)}{2}+1\equiv 0,1,2,3,4,6,8,9,12,13,16,18 \pmod{23},$$

which gives us congruences for the omitted ones, namely

$$\tau(23n+\alpha)\equiv 0 \pmod{23} \quad \text{for } \alpha=5,7,10,11,14,15,17,19,20,21,22.$$

The α's are the quadratic non-residues.

Modulus 2. Again,

$$q\,\theta(q)^{24} \;\equiv\; q\,\theta(q^{(2^3)})^3 \pmod{2},$$

so we immediately see that

$$\tau(8n+\alpha)\equiv 0 \pmod{2} \quad \text{for } \alpha\not\equiv 1 \bmod 8.$$

In particular,

$$\tau(2n)\equiv 0 \pmod{2}.$$

In fact, more can be said by using Jacobi's identity as for the modulus 7,

$$q\,\theta(q^8)^3=q\sum_{n\geqslant 0}(-1)^n\,(2n+1)q^{4n(n+1)}=\sum_{n\geqslant 0}(-1)^n\,(2n+1)q^{(2n+1)^2}.$$

This shows that

$$\tau(n)\equiv 1 \pmod{2} \quad\Longleftrightarrow\quad n \text{ is an odd square.}$$

Modulus 3. Here,

$$q\,\theta(q)^{24} \;\equiv\; q\,\theta(q^3)^8 \pmod{3},$$

and we see that only exponents of the form $3n+1$ will appear. So

$$\tau(3n),\ \tau(3n+2)\equiv 0 \pmod{3}. \tag{1}$$

2 A Glance at the Theory of Modular Forms

2.1 Basics About Modular Forms

The group

$$\mathrm{SL}(2,\mathbb{R})=\left\{A\in\mathbb{R}^{2\times 2}\colon\ \det A=1\right\}$$

acts on the upper half plane $\mathcal{H}=\{\omega\in\mathbb{C}\colon\ \operatorname{im}\omega>0\}$ via

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\cdot\omega=\frac{a\,\omega+b}{c\,\omega+d}.$$

Let's consider the discrete subgroup SL(2, $\mathbb{Z}$) made up of such matrices with integer entries. This group is generated by the two elements

$$T=\begin{pmatrix} 1 & 1\\ & 1\end{pmatrix},\quad S=\begin{pmatrix} & 1\\ -1 & \end{pmatrix}.$$

Definition 2. *A function $f:\mathcal{H}\to\mathbb{C}$ is called a modular form of weight k if*

$$f\left(\frac{a\,\omega+b}{c\,\omega+d}\right)=(c\,\omega+d)^k\,f(\omega),$$

and f is analytic at ∞.

We only have to check

$$f(\omega+1)=f(\omega),\quad f(-1/\omega)=\omega^k\,f(\omega).$$

The fact that a modular form f is periodic with period 1 and analytic at ∞ implies that it has an expansion in $q=e^{2\pi i\omega}$ convergent for all $|q|<1$,

$$f(q)=\sum_{n\geqslant 0}a_n\,q^n.$$

Note that modular forms of odd weight have to be zero. However, the concept of odd weight will make more sense when considering subgroups of $\mathrm{SL}(2,\mathbb{Z})$ instead of the full group.

Definition 3. *A modular form f is called a cusp form if it vanishes at ∞, that is the Fourier coefficient $a_0=0$.*

The simplest examples of modular forms are given by the Eisenstein series

$$G_k(\omega)=\sum_{(m,n)\neq 0}\frac{1}{(m+n\,\omega)^k},$$

which converge absolutely when $k>2$. Note that terms are cancelling for k odd so that we constantly end up with 0. It is easy to see that G_{2k} for $k>1$ is indeed a modular form of weight $2k$. Since

$$G_{2k}(\infty)=\sum_{m\neq 0}\frac{1}{m^{2k}}=2\,\zeta(2k),$$

we often consider the normalized Eisenstein series

$$E_k=\frac{G_{2k}}{2\,\zeta(2k)}.$$

Definition 4. *Let's introduce the sum of divisors functions*

$$\sigma_k(n)\triangleq\sum_{d\,|\,n}d^k.$$

The functions σ_k are multiplicative and hence determined by

$$\sigma_k(p^\alpha)=1+p^k+p^{2k}+\ldots+p^{\alpha k}$$

for primes p.

Lemma 5. *We have*

$$E_k=\frac{G_{2k}}{2\,\zeta(2k)}=1-\frac{4k}{B_{2k}}\sum_{n\geqslant 1}\sigma_{2k-1}(n)\,q^n,$$

where B_k are the Bernoulli numbers defined by

$$\frac{x}{e^x-1}=\sum_{n\geqslant 0} B_n \frac{x^n}{n!}.$$

Note that by reordering,

$$\begin{aligned}\sum_{n\geqslant 1} \sigma_k(n)\, q^n &= \sum_{n\geqslant 1}\sum_{d\,|n} d^k q^n \\ &= \sum_{d\geqslant 1} d^k \left(q^d+q^{2d}+q^{3d}\ldots\right) \\ &= \sum_{n\geqslant 1} n^k \frac{q^n}{1-q^n}.\end{aligned}$$

This provides the so called Lambert series for E_k, namely

$$E_k=\frac{G_{2k}}{2\,\zeta(2k)}=1-\frac{4k}{B_{2k}}\sum_{n\geqslant 1}\frac{n^k q^n}{1-q^n}.$$

2.2 Spaces of Modular Forms

Definition 6. *Let $\mathcal{M}_n$ denote the space of all modular forms of weight $2n$.*

The following fundamental lemma, see [McKean and Moll, 1999], is crucial for describing the spaces $\mathcal{M}_n$.

Lemma 7. *Let f be a modular form of weight $2n$, $f\neq 0$. Denote with m_ρ, m_i, m_∞ the multiplicities with which f vanishes at ρ, i, ∞, and let m be the sum of multiplicities of all the other roots in the fundamental cell. Then*

$$\frac{1}{3}m_\rho+\frac{1}{2}m_i+m_\infty+m=\frac{1}{6}n.$$

Corollary 8. *$\mathcal{M}_n$ is a finite dimensional linear space, spanned by the independent forms*

$$E_2^a\,E_3^b,\quad 2a+3b=n.$$

In particular,

$$\dim \mathcal{M}_n=\begin{cases}\lfloor\frac{n}{6}\rfloor & n\equiv 1 \pmod 6\\ \lfloor\frac{n}{6}\rfloor+1 & \text{otherwise.}\end{cases}$$

2.3 Explicit Examples

For illustration and future use, we give some explicit examples.

$$\begin{aligned}\mathcal{M}_0 &= \mathbb{C}\\ \mathcal{M}_1 &= \{0\}\\ \mathcal{M}_2 &= \mathbb{C}\,E_2\\ \mathcal{M}_3 &= \mathbb{C}\,E_3\\ \mathcal{M}_4 &= \mathbb{C}\,E_2^2\\ \mathcal{M}_5 &= \mathbb{C}\,E_2E_3\\ \mathcal{M}_6 &= \mathbb{C}\,E_2^3\oplus\mathbb{C}\,\Delta\\ \mathcal{M}_7 &= \mathbb{C}\,E_2^2E_3\\ \mathcal{M}_8 &= \mathbb{C}\,E_2^4\oplus\mathbb{C}\,\Delta\end{aligned}$$

Also recall that

$$E_k = 1 - \frac{4k}{B_{2k}} \sum_{n \geqslant 1} \sigma_{2k-1}(n)\, q^n,$$

and let's use this to write down the first terms of the Fourier expansions

$$\begin{aligned}
E_1 &= 1 - 24 \sum_{n \geqslant 1} \sigma_1(n)\, q^n &&= 1 - 24q - 72q^2 - 96q^3 - 168q^4 - \ldots \\
E_2 &= 1 + 240 \sum_{n \geqslant 1} \sigma_3(n)\, q^n &&= 1 + 240q + 2160q^2 + 6720q^3 + \ldots \\
E_3 &= 1 - 504 \sum_{n \geqslant 1} \sigma_5(n)\, q^n &&= 1 - 504q - 16632q^2 - 122976q^3 - \ldots \\
E_4 &= 1 + 480 \sum_{n \geqslant 1} \sigma_7(n)\, q^n &&= 1 + 480q + 61920q^2 + 1050240q^3 + \ldots \\
E_5 &= 1 - 264 \sum_{n \geqslant 1} \sigma_9(n)\, q^n &&= 1 - 264q - 135432q^2 - 5196576q^3 - \ldots \\
E_6 &= 1 + \frac{65520}{691} \sum_{n \geqslant 1} \sigma_{11}(n)\, q^n &&= 1 + \frac{65520}{691} q + \frac{134250480}{691} q^2 + \ldots \\
\Delta &= \sum_{n \geqslant 1} \tau(n)\, q^n &&= q - 24q^2 + 252q^3 - 1472q^4 + \ldots
\end{aligned}$$

Remark 9. In the sequel we will consider congruences mod p for the numbers $\tau(n)$ by establishing relationships between the Eisenstein series E_n and Ramanujan's Δ. It seems that the following is true

$$2m \equiv 2n \pmod{p-1} \quad \Longrightarrow \quad E_m \equiv E_n \pmod{p},$$

where we also allow $m, n = 0$ with the convention that $E_0 = 1$. In each individual case this is easily verified but I didn't find a proof or a reference for the general case. Note that the statement above really comes down to divisibility properties of the Bernoulli numbers.

2.4 Differentiating Modular Forms

When introducing the Eisenstein series

$$E_k(\omega) = \frac{1}{2\,\zeta(2k)} \sum_{(m,n) \neq 0} \frac{1}{(m + n\,\omega)^{2k}},$$

we started with the assumption that $k \geqslant 2$ in order for the defining sums to converge. But after rewriting the sums in terms of σ_{2k-1} or as Lambert series our hopes are raised to also find that E_1 has some modular properties. As it turns out, see [Beukers, 2007], the function E_1 defined by

$$E_1 = 1 - 24 \sum_{n \geqslant 1} \sigma_1(n)\, q^n = 1 - 24 \sum_{n \geqslant 1} \frac{n\, q^n}{1 - q^n}$$

is indeed close to being modular of weight 2 (recall that such a form cannot exist). While E_1 does not satisfy $E_1(-1/z) = z^2 E_1(z)$ it does satisfy

$$E_1(-1/z) = z^2 E_1(z) + \frac{12}{2\pi i}\, z.$$

E_1 still plays an important role, for instance when it comes to differentiating modular forms. As before $q = e^{2\pi i z}$. Since

$$\frac{\mathrm{d}z}{\mathrm{d}q} = \frac{1}{2\pi i\, q},$$

we have

$$\theta f \triangleq q \frac{\mathrm{d}f}{\mathrm{d}q} = \frac{1}{2\pi i} \frac{\mathrm{d}f}{\mathrm{d}z}.$$

The following lemma is due to Ramanujan, see [Serre, 1971].

Lemma 10. *If f is a modular form of weight k then*

$$\theta f - \frac{k}{12} E_1 f$$

is a modular form of weight $k+2$.

Remark 11. Ramanujan also discovered, see [Beukers, 2007], that the pseudoform E_1 of weight 2 when treated the same behaves similar.

$$\theta E_1 - \frac{2}{12} E_1^2 = -\frac{1}{12}\left(E_2 + E_1^2\right),$$

that is

$$\theta E_1 = \frac{1}{12}\left(E_1^2 - E_2\right). \tag{2}$$

To put it in a fancy way, the ring $\mathbb{C}[E_1, E_2, E_3]$ is closed under differentiation. Recall that the ring of modular forms is just $\mathbb{C}[E_2, E_3]$.

Note that the above identity is equivalent to the mysteriously looking

$$\sigma_1(n) - 6n\,\sigma_1(n) - 12\,\sigma_1 * \sigma_1(n) + 5\,\sigma_3(n) = 0.$$

Remark 12. The pseudoform E_1 is the logarithmic derivative of

$$\Delta \triangleq q \prod_{n \geqslant 1} (1-q^n)^{24},$$

meaning that

$$\begin{aligned}
\theta(\log \Delta) &= \frac{1}{2\pi i} \frac{\mathrm{d}}{\mathrm{d}z} (\log \Delta) \\
&= \frac{1}{2\pi i} \frac{\mathrm{d}}{\mathrm{d}z} \left(2\pi i\, z + 24 \sum_{n \geqslant 1} \log(1-q^n) \right) \\
&= 1 - 24 \sum_{n \geqslant 1} \frac{n\, q^n}{1-q^n} \\
&= E_1(z).
\end{aligned}$$

Together with the transformation rule for E_1 this can be employed, see [Serre, 1971], to easily prove that Δ as defined above is a modular form of weight 12.

2.5 Hecke Operators

Hecke introduced certain commuting operators $T_n \colon \mathcal{M}_k \to \mathcal{M}_k$ on the spaces of modular forms. The T_n map cusp forms to cusp forms, and whenever a cusp form is a simultanuous eigenform for these operators this implies nice properties like an Euler product expansion. Since Δ is the only cusp form of weight 12 it is automatically an eigenform and the general theory provides the following properties.

$$\begin{aligned}
\tau(m\,n) &= \tau(m)\,\tau(n) \quad \text{if } \gcd(m,n) = 1, \\
\tau(p^{n+1}) &= \tau(p)\,\tau(p^n) - p^{11}\,\tau(p^{n-1}) \quad \text{if } p \text{ prime}.
\end{aligned}$$

It is remarkable that this and more was conjectured by Ramanujan long before the general theory. These properties are also captured in the following Euler product expansion for the Dirichlet series attached to $\tau(n)$, namely

$$L_\tau(s) = \sum_{n \geqslant 1} \frac{\tau(n)}{n^s} = \prod_p 1 + \sum_{n \geqslant 1} \frac{\tau(p^n)}{p^{n\,s}} = \prod_p \frac{1}{1 - \tau(p)\,p^{-s} + p^{11-2s}}.$$

Example 13. The above multiplicative features of $\tau(n)$ show that

$$\tau(p) \equiv 0 \pmod p \quad \Longrightarrow \quad \tau(n\,p) \equiv 0 \pmod p.$$

With this insight it follows for instance immediately from $\tau(3) = 252$ that

$$\tau(3n) \equiv 0 \pmod 3$$

as we showed before, see (1). There are, however, only a handful known primes p dividing $\tau(p)$. In (5) we list the first few such primes as $2, 3, 5, 7, 2411$.

Example 14. The multiplicative properties further imply that

$$\tau(n\,p) \equiv \tau(n)\,\tau(p) \pmod p.$$

For instance $\tau(23) \equiv 1 \pmod{23}$, and hence

$$\tau(23n) \equiv \tau(n) \pmod{23}.$$

Remark 15. Ramanujan also conjectured the following bound

$$|\tau(p)| \leqslant 2\,p^{11/2},$$

which was finally proved in 1973 based on a proof of the Weil conjectures by Deligne (he worked on the Riemann hypothesis for varieties over finite fields, and was awarded the Fields medal for this work). As of 2005, the above inequality held the world record for the ratio length of proof/length of the statement, see [Dalawat, 2006]. In general,

$$|\tau(n)| \leqslant \sigma_0(n)\,n^{11/2} = n^{11/2+o(1)}.$$

3 Computing $\tau(n)$

3.1 Exact Formulas

Let's derive some formulas for Δ. We will employ the following short-hand notation

$$\varphi * \psi(n) \triangleq \sum_{m=0}^{n} \varphi(m)\,\psi(n-m).$$

Throughout, we will make heavy use of the explicit presentations given in section 2.3.

Using E_2^3, E_3^2. We want to write

$$\Delta = \alpha\,E_2^3 + \beta\,E_3^2.$$

Equating coefficients of the first two terms in the q-expansions yields

$$\begin{aligned} 0 &= \alpha + \beta, \\ 1 &= 3 \cdot 240\alpha - 2 \cdot 504\beta. \end{aligned}$$

Thus

$$1728\,\Delta = E_2^3 - E_3^2,$$

and

$$\tau(n) = \frac{5}{12}\sigma_3(n) + 100\,\sigma_3 * \sigma_3(n) + 8000\,\sigma_3 * \sigma_3 * \sigma_3(n) + \frac{7}{12}\sigma_5(n) - 147\,\sigma_5 * \sigma_5(n).$$

Using E_3^2, E_6. Now, lets find α, β such that

$$\Delta = \alpha\, E_3^2 + \beta\, E_6.$$

This requires

$$\begin{aligned} 0 &= \alpha + \beta, \\ 1 &= -2 \cdot 504\alpha + \frac{65520}{691}\beta. \end{aligned}$$

Hence

$$762048\,\Delta = -691\, E_3^2 + 691\, E_6,$$

or

$$\tau(n) = \frac{691}{756}\sigma_5(n) - \frac{691}{3}\sigma_5 * \sigma_5(n) + \frac{65}{756}\sigma_{11}(n). \tag{3}$$

Using $E_6, \theta E_5$. From lemma 10 we know that

$$\theta E_5 - \frac{5}{6}\, E_1\, E_5 = -\frac{5}{6} - 24q + \ldots$$

is a modular form of weight 12.

$$\Delta = \alpha\, E_6 + \beta\left(\theta E_5 - \frac{5}{6}\, E_1\, E_5\right)$$

yields to

$$\begin{aligned} 0 &= \alpha - \frac{5}{6}\beta, \\ 1 &= \frac{65520}{691}\alpha - 24\,\beta. \end{aligned}$$

We conclude that

$$228096\,\Delta = 3455\, E_6 + 4146\,\theta E_5 - 3455\, E_1\, E_5,$$

and

$$\tau(n) = \frac{2275}{1584}\sigma_{11}(n) - \frac{691}{144}\,n\,\sigma_9(n) + \frac{3455}{9504}\,\sigma_1(n) + \frac{3455}{864}\,\sigma_9(n) - \frac{3455}{36}\,\sigma_1 * \sigma_9(n). \tag{4}$$

Among what we found, (4.1.3) is probably the most useful formula for actually computing $\tau(n)$. Expanded it reads as

$$\tau(n) = \frac{65}{756}\sigma_{11}(n) + \frac{691}{756}\sigma_5(n) - \frac{691}{3}\sum_{m=1}^{n} \sigma_5(m)\,\sigma_5(n-m).$$

3.2 Recurrences

Using lemma 10 we find that

$$\theta\,\Delta - E_1\,\Delta = 0,$$

since there is no nonzero cusp form of weight 14. Thus

$$(n-1)\,\tau(n) = -24\,\sigma_1 * \tau(n) = -24\sum_{m=1}^{n-1}\tau(m)\,\sigma_1(n-m),$$

which is a recursion for $\tau(n)$.

As a nice by-product, we also find that

$$n \equiv 0, 2 \pmod 6 \quad \Longrightarrow \quad \tau(n) \equiv 0 \pmod{24}.$$

4 Congruences for $\tau(n)$

The results in this section are mostly in the spirit of Ramanujan, see [Berndt and Ono, 1999]. For more congruences and a glimpse at a general theory behind these congruences we refer the reader to [Swinnerton-Dyer, 1988].

Modulus 5. Note that

$$E_2 \equiv 1, \quad E_3 \equiv E_1 \pmod 5.$$

Thus with (2),

$$1728\,\Delta = E_2^3 - E_3^2 \equiv E_2 - E_1^2 = -12\,\theta E_1 \pmod 5,$$

or

$$\tau(n) \equiv n\,\sigma_1(n) \pmod 5.$$

Note that this also follows immediately from (4).

Modulus 25. Using again $E_2 \equiv 1 \pmod 5$ and $E_3 \equiv E_1 \pmod 5$, we get

$$\begin{aligned} 1728\,\Delta &= E_2^3 - E_3^2 \\ &= 2\,(E_2^2 - E_1\,E_3) - (E_2 - E_1^2) + E_2\,(E_2-1)^2 - (E_3 - E_1)^2 \\ &\equiv 2\,(E_2^2 - E_1\,E_3) - (E_2 - E_1^2) \pmod{25} \\ &= -4\,\theta E_3 + 12\,\theta E_1 \end{aligned}$$

which together means

$$\tau(n) \equiv 4n\,\sigma_1(n) - 3n\,\sigma_5(n) \pmod{25}.$$

The polynomial

$$x^2\,(x^4-1)^2 = x\left(x^9 - 2\,x^5 + x\right)$$

vanishes for all moduli with respect to 25, which implies that

$$n\,\sigma_9(n) - 2n\,\sigma_5(n) + n\,\sigma_1(n) \equiv 0 \pmod{25}.$$

Together with the obvious $\sigma_5(n) \equiv \sigma_1(n) \pmod 5$ this simplifies our congruence to

$$\tau(n) \equiv n\,\sigma_9(n) \pmod{25}.$$

Modulus 5^k. Ramanujan conjectured, see [Berndt and Ono, 1999], that for any k it is possible to find a, b such that if n is not a multiple of 5

$$\tau(n) \equiv n^a \, \sigma_b(n) \pmod{5^k}.$$

He offers for example

$$\tau(n) \equiv n^{41} \, \sigma_{29}(n) \pmod{125}$$

whenever n is not a multiple of 5. While the latter is indeed true, the conjecture is false for $k \geqslant 4$. To see this take $n = 443$, which is prime, and verify that for any a, b

$$\tau(443) = 328369848718692 \equiv 567 \not\equiv 443^a \left(1 + 443^b\right) \pmod{5^4}$$

since $443^2 \equiv -1 \pmod{5^4}$. It's comforting to know that even a genius like Ramanujan can err.

Modulus 7. Clearly,

$$E_3 \equiv 1, \quad E_2^2 = E_4 \equiv E_1 \pmod{7}.$$

Therefore lemma 10 gives,

$$1728 \, \Delta = E_2^3 - E_3^2 \equiv E_1 \, E_2 - E_3 = 3 \, \theta E_2 \pmod{7},$$

that is

$$\tau(n) \equiv n \, \sigma_3(n) \pmod{7}.$$

Modulus 691. It follows right from the exact formula (3),

$$\tau(n) = \frac{691}{756} \sigma_5(n) - \frac{691}{3} \sigma_5 * \sigma_5(n) + \frac{65}{756} \sigma_{11}(n),$$

that

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}.$$

5 Negative Results

As presented in [Serre, 1997], congruences such as we showed for modulus 3, see (1),

$$m \equiv 2 \pmod{3} \quad \Longrightarrow \quad \tau(m) \equiv 0 \pmod{3},$$

don't necessarily exist. In fact, for instance no congruence of the form

$$m \equiv a \pmod{b} \quad \Longrightarrow \quad \tau(m) \equiv c \pmod{11}$$

can exist for any integers a, b, c such that a, b are relatively prime.

6 Almost Always Divisibility

Ramanujan asserted, see [Rankin, 1988], that for

$$p = 3, 5, 7, 23, 691,$$

$\tau(n)$ is almost always divisible by p in the sense that

$$\sum_{n \leqslant x \, , \, p \nmid \tau(n)} 1 = o(x).$$

In fact, he claims that for almost all n

$$\tau(n) \equiv 0 \pmod{2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 23 \cdot 691},$$

which he contrasts to the fact that $n = 1381$ is the first such that $\tau(n) \equiv 0 \pmod{691}$.

Today it is known that for any integer m, $\tau(n)$ is almost always divisible by m. But the proof of this fact requires different methods than Ramanujan used to show his assertions.

7 Open Problems

Does $\tau(n)$ ever vanish, that is $\tau(n) = 0$ for some n? This is known as Lehmer's conjecture and has been empirically verified for large values of n. As initially stated, one hoped that Lehmer's conjecture might be attackable by congruence considerations. To illustrate this hope, consider just the congruence

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}.$$

Rewritten as

$$\tau(p) \equiv 1 + p^{11} \pmod{691}$$

it shows that

$$\tau(p) = 0 \implies p \equiv -1 \pmod{691},$$

because $\mathbb{Z}_{690}$ contains no elements of order 22. The first candidates are thus

$$p = 1381, 5527, 8291, 12437, 22111, 29021, 30403, \ldots$$

Combining this with other congruences one is able to quite impressively narrow the density of these candidates, see [Serre, 1997]. Let's just consider the other congruences we found, namely

$$\begin{aligned} \tau(p) &\equiv p\,(1 + p^9) \pmod{25} \\ \tau(p) &\equiv p\,(1 + p^3) \pmod{7}. \end{aligned}$$

Then

$$\tau(p) = 0 \implies \left\{ \begin{array}{l} p \equiv -1 \pmod{5^2 \cdot 691} \\ p \equiv -1, 3, 5 \pmod{7} \end{array} \right\},$$

which leaves us with the candidates

$$p = 863749, 1381999, 1589299, 1692949, 2314849, 2833099, \ldots$$

The only primes p known for which

$$\tau(p) \equiv 1 \pmod{p}$$

are $p = 11, 23, 691$. It is an open problem, see [Sloane, 2007], to decide whether there are more such primes or even infinitely many. None are known up to 314747.

The following results have been verified for all primes $\leqslant 16091$.

$$\begin{aligned} \tau(p) \equiv 0 \pmod{p} &\implies p = 2, 3, 5, 7, 2411, \ldots \\ \tau(p) \equiv 1 \pmod{p} &\implies p = 11, 23, 691, \ldots \\ \tau(p) \equiv -1 \pmod{p} &\implies p = 5807, \ldots \end{aligned} \tag{5}$$

Is $\tau(n)$ ever a prime? The first number such that this is the case is

$$\tau(63001) = \tau(251^2) = \tau(251)^2 - 251^{11} = -805616635278024062573217 47,$$

as found in [Lehmer, 1965].

Bibliography

[Berndt and Ono, 1999] Berndt, B. C. and Ono, K. (1999). Ramanujan's unpublished manuscript on the partition and τ functions with proofs and commentary. *Seminaire Lotharingien de Combinatoire*, 42(c).

[Beukers, 2007] Beukers, F. (2007). Modular forms. Published online at http://www.math.uu.nl/people/beukers/modularforms/modularformscript.pdf.

[Dalawat, 2006] Dalawat, C. S. (2006). The tao of mathematics, and think locally. Published online at http://arxiv.org/abs/math/0605327.

[Lehmer, 1965] Lehmer, D. H. (1965). The primality of Ramanujan's τ-function. *The American Mathematical Monthly*, 72(2):15–18.

[McKean and Moll, 1999] McKean, H. and Moll, V. (1999). *Elliptic Curves: Function Theory, Geometry, Arithmetic*. Cambridge University Press.

[Rankin, 1988] Rankin, R. A. (1988). τ-function and its generalizations. In *Ramanujan Revisited, Proceedings of the Cenetary Conference*. Academic Press.

[Serre, 1971] Serre, J.-P. (1971). Congruences and modular forms (following H.P.F. Swinnerton-Dyer). *Séminaire Bourbaki*, (416). Translated by Jay Pottharst.

[Serre, 1997] Serre, J.-P. (1997). An interpretation of some congruences concerning Ramanujan's τ-function. Published online at http://www.rzuser.uni-heidelberg.de/ hb3/serre.ps.

[Sloane, 2007] Sloane, N. J. A. (2007). The On-Line Encyclopedia of Integer Sequences. Published electronically at http://www.research.att.com/sequences.

[Swinnerton-Dyer, 1988] Swinnerton-Dyer, H. P. F. (1988). Congruence properties of $\tau(n)$. In *Ramanujan Revisited, Proceedings of the Cenetary Conference*. Academic Press.