A Dirichlet Series for the Congruent Number Problem

Thomas A. Hulse
Boston College

Joint work with Chan Ieong Kuan, David Lowry-Duda and Alexander Walker

Université Laval
Conférence de théorie des nombres
Québec-Maine

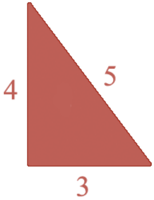
6 October 2018

Congruent Number Problem

As the name suggests, a **rational right triangle** is a right triangle where all three side lengths are rational.

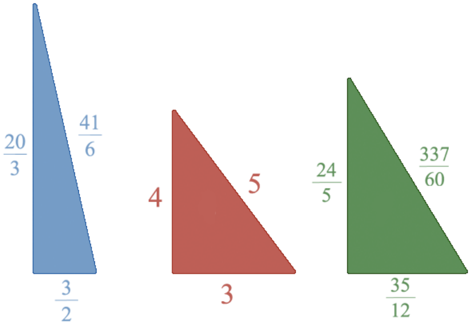
Congruent Number Problem

As the name suggests, a **rational right triangle** is a right triangle where all three side lengths are rational.



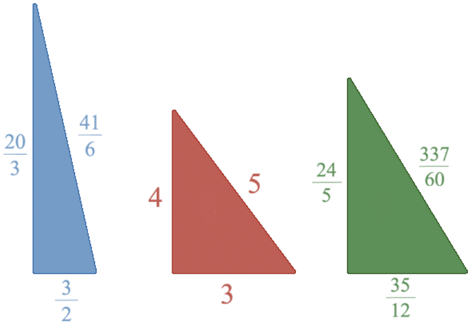
Congruent Number Problem

As the name suggests, a **rational right triangle** is a right triangle where all three side lengths are rational.



Congruent Number Problem

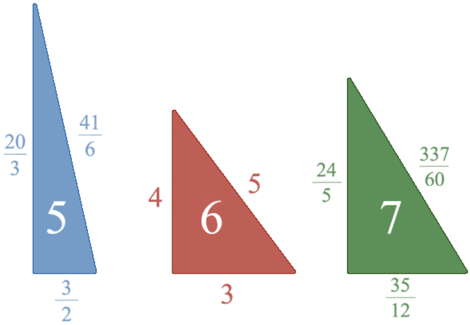
As the name suggests, a **rational right triangle** is a right triangle where all three side lengths are rational.



We say that the natural number n is a **congruent number** if it is the area of a rational right triangle.

Congruent Number Problem

As the name suggests, a **rational right triangle** is a right triangle where all three side lengths are rational.



We say that the natural number n is a **congruent number** if it is the area of a rational right triangle.

This leads to a natural question:

This leads to a natural question:

Question (The Congruent Number Problem)

Given $n \in \mathbb{N}$, is there a terminating algorithm, whose duration depends on the size of n, that will determine if n is a congruent number?

This leads to a natural question:

Question (The Congruent Number Problem)

Given $n \in \mathbb{N}$, is there a terminating algorithm, whose duration depends on the size of n, that will determine if n is a congruent number?

From the previous slide, we know that 5,6,7 are congruent numbers. The 17th Century French lawyer, Pierre de Fermat, was the first mathematician to prove that 1 is *not* a congruent number.

This leads to a natural question:

Question (The Congruent Number Problem)

Given $n \in \mathbb{N}$, is there a terminating algorithm, whose duration depends on the size of n, that will determine if n is a congruent number?

From the previous slide, we know that 5,6,7 are congruent numbers. The 17th Century French lawyer, Pierre de Fermat, was the first mathematician to prove that 1 is *not* a congruent number.

This is the only complete proof Fermat ever wrote, published posthumously, and it uses the technique of infinite descent.

This leads to a natural question:

Question (The Congruent Number Problem)

Given $n \in \mathbb{N}$, is there a terminating algorithm, whose duration depends on the size of n, that will determine if n is a congruent number?

From the previous slide, we know that 5,6,7 are congruent numbers. The 17th Century French lawyer, Pierre de Fermat, was the first mathematician to prove that 1 is *not* a congruent number.

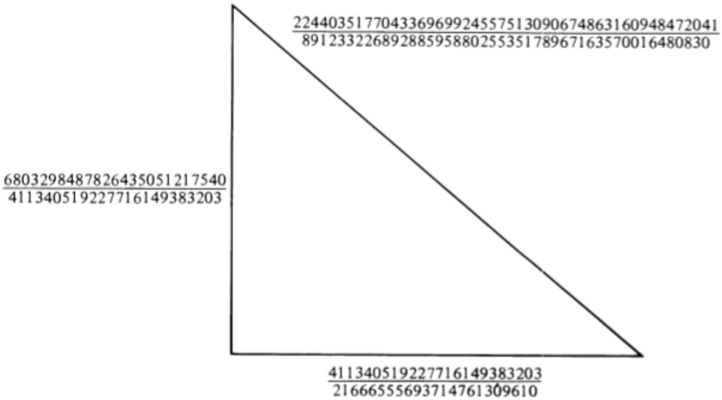
This is the only complete proof Fermat ever wrote, published posthumously, and it uses the technique of infinite descent.

There is a known (awful) way to find out if n is a congruent number, if it is indeed a congruent number. We can take the parametrization of primitive pythagorean triples due to Euclid and then wait until our congruent number shows up.

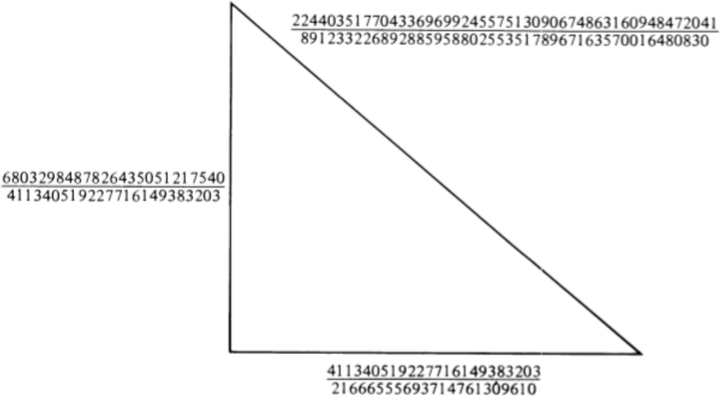
How long might this algorithm take to find a given congruent number?

How long might this algorithm take to find a given congruent number?
A long time.

How long might this algorithm take to find a given congruent number?
A long time.



How long might this algorithm take to find a given congruent number?
A long time.



This is the simplest rational right triangle with area 157, discovered by Don Zagier around 1990.[2]

There are ways to simplify and reformulate this problem. Indeed, rational triangles scaled by an integer multiple are still rational.

There are ways to simplify and reformulate this problem. Indeed, rational triangles scaled by an integer multiple are still rational.

Observation

The square-free integer t is a congruent number if and only if it is the square-free part of $xy/2$ where $(x, y, z) \in \mathbb{Z}^3$ is a primitive Pythagorean triple, that is $x^2 + y^2 = z^2$ and x, y, z are pairwise coprime.

A criterion for determining t's congruency already exists, it just hasn't been completely proven to always work. (probably does)

A criterion for determining t's congruency already exists, it just hasn't been completely proven to always work. (probably does)

Theorem (Tunnell, 1983[2])

Let t be an odd square-free natural number. Consider the two conditions:

(A) *t is congruent;*

(B) *the number of triples of integers (x, y, z) satisfying $2x^2 + y^2 + 8z^2 = t$ is equal to twice the number of triples satisfying $2x^2 + y^2 + 32z^2 = t$.*

Then (A) implies (B); and, if a weak form of the Birch-Swinnerton-Dyer conjecture is true, then (B) also implies (A).

A criterion for determining t's congruency already exists, it just hasn't been completely proven to always work. (probably does)

Theorem (Tunnell, 1983[2])

Let t be an odd square-free natural number. Consider the two conditions:

(A) *t is congruent;*

(B) *the number of triples of integers (x, y, z) satisfying $2x^2 + y^2 + 8z^2 = t$ is equal to twice the number of triples satisfying $2x^2 + y^2 + 32z^2 = t$.*

Then (A) implies (B); and, if a weak form of the Birch-Swinnerton-Dyer conjecture is true, then (B) also implies (A).

A similar but different criterion holds if t is even.

A criterion for determining t's congruency already exists, it just hasn't been completely proven to always work. (probably does)

Theorem (Tunnell, 1983[2])

Let t be an odd square-free natural number. Consider the two conditions:

(A) *t is congruent;*

(B) *the number of triples of integers (x, y, z) satisfying $2x^2 + y^2 + 8z^2 = t$ is equal to twice the number of triples satisfying $2x^2 + y^2 + 32z^2 = t$.*

Then (A) implies (B); and, if a weak form of the Birch-Swinnerton-Dyer conjecture is true, then (B) also implies (A).

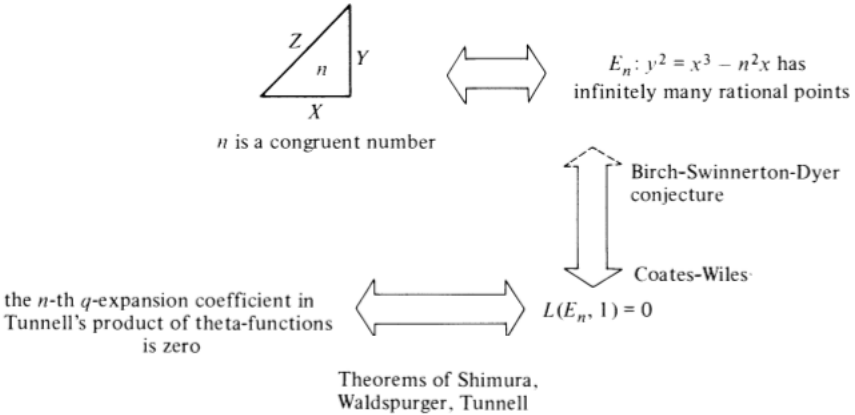
A similar but different criterion holds if t is even.

We see that if (B) does imply (A), then all we have to do is perform a search that would take a computable, finite amount of time that depends on the size of t. This would be an acceptable solution to the Congruent Number Problem.

Why the heck would this work?

Why the heck would this work?

Here's a helpful diagram made by Koblitz[2]:



There is an alternate way to formulate the congruent number problem concerning arithmetic progressions of squares.

There is an alternate way to formulate the congruent number problem concerning arithmetic progressions of squares.

Theorem

The natural number h is a congruent number if and only if there exists $r \in \mathbb{Q}$ such that $(r^2 \pm h)$ are squares of elements in $\mathbb{Q}$.

There is an alternate way to formulate the congruent number problem concerning arithmetic progressions of squares.

Theorem

The natural number h is a congruent number if and only if there exists $r \in \mathbb{Q}$ such that $(r^2 \pm h)$ are squares of elements in $\mathbb{Q}$.

That is, h is a congruent number if and only if we have an arithmetic progression of rational squares: $q - h, q, q + h$.

There is an alternate way to formulate the congruent number problem concerning arithmetic progressions of squares.

Theorem

The natural number h is a congruent number if and only if there exists $r \in \mathbb{Q}$ such that $(r^2 \pm h)$ are squares of elements in $\mathbb{Q}$.

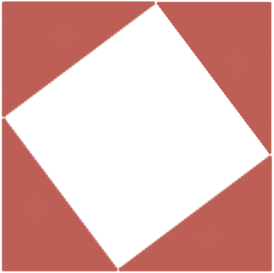
That is, h is a congruent number if and only if we have an arithmetic progression of rational squares: $q - h, q, q + h$.

By scaling, we see equivalently that square-free t is a congruent number if and only if there are natural numbers $m, n \in \mathbb{N}$ such that $(m - tn), m, (m + tn)$, and n are all squares.

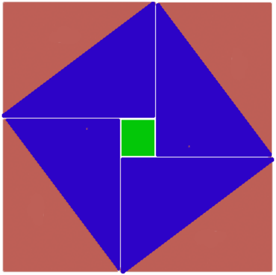
Proof of equivalence:

Proof of equivalence: Suppose we have a rational right triangle:

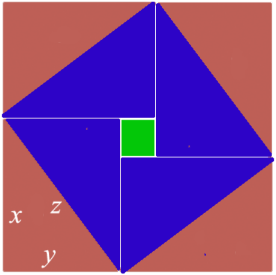
Proof of equivalence: We can make two squares by doing this.



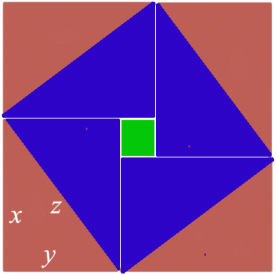
Proof of equivalence: And we can make a smaller square by doing this.



Proof of equivalence: Now we label the relevant quantities.

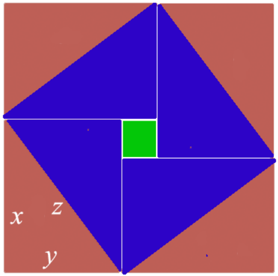


Proof of equivalence:



By our hypothesis, $x, y, z \in \mathbb{Q}$. We see that each of the above squares are rational, with side lengths $(x + y), z$ and $(x - y)$ in descending order, and that the difference in area between subsequent squares are the triangles, which we can say have area $n \in \mathbb{N}$.

Proof of equivalence:



By our hypothesis, $x, y, z \in \mathbb{Q}$. We see that each of the above squares are rational, with side lengths $(x+y), z$ and $(x-y)$ in descending order, and that the difference in area between subsequent squares are the triangles, which we can say have area $n \in \mathbb{N}$.

Multiplying by a factor of $\frac{1}{2}$ we see $(z/2)^2 \pm n$ are both squares. This argument is reversible.

Shifted Sums

Let $s : \mathbb{N} \to \{0, 1\}$ be the square indicator function where

$$s(n) := \begin{cases} 0 & \text{if } n \text{ is not a square} \\ 1 & \text{if } n \text{ is a square} \end{cases}$$

Shifted Sums

Let $s : \mathbb{N} \to \{0, 1\}$ be the square indicator function where

$$s(n) := \begin{cases} 0 & \text{if } n \text{ is not a square} \\ 1 & \text{if } n \text{ is a square} \end{cases}$$

With this we can reformulate the "arithmetic progression of squares" argument to be that square-free t is congruent if and only if:

$$s(m-n)s(m)s(m+n)s(tn) \neq 0$$

for some $m, n \in \mathbb{N}$.

Shifted Sums

Let $s : \mathbb{N} \to \{0, 1\}$ be the square indicator function where

$$s(n) := \begin{cases} 0 & \text{if } n \text{ is not a square} \\ 1 & \text{if } n \text{ is a square} \end{cases}$$

With this we can reformulate the "arithmetic progression of squares" argument to be that square-free t is congruent if and only if:

$$s(m-n)s(m)s(m+n)s(tn) \neq 0$$

for some $m, n \in \mathbb{N}$.

Or alternately, a square-free t is congruent if any only if the double partial sum

$$S_t(X) = \sum_{n,m<X} s(m-n)s(m)s(m+n)s(tn)$$

is not the constant zero function.

It turns out we can make a more precise statement.

It turns out we can make a more precise statement.

Theorem (H., Kuan, Lowry-Duda, Walker)

Let $t \in \mathbb{N}$ be squarefree, and let $s(n)$ be the square-indicator function. Let r be the rank of the elliptic curve $E_t : y^2 = x^3 - t^2 x$ over $\mathbb{Q}$. For $X > 1$, we have the asymptotic expansion:

$$S_t(X) := \sum_{m,n<X} s(m+n)s(m-n)s(m)s(tn) = C_t X^{\frac{1}{2}} + O_t((\log X)^{r/2}).$$

in which $C_t := \sum_{h \in \mathcal{H}(t)} \frac{1}{h}$ is the convergent sum over $\mathcal{H}(t)$, the set of hypotenuses, h, of dissimilar primitive right triangles with squarefree part of the area t.

Proof Outline: From the construction of the arithmetic progression of squares from a right triangle, we have that $m^2 \pm tn^2$ are squares when $m \in H(t)$ and n relates to the area of the triangle so we see that

Proof Outline: From the construction of the arithmetic progression of squares from a right triangle, we have that $m^2 \pm tn^2$ are squares when $m \in H(t)$ and n relates to the area of the triangle so we see that

$$\begin{aligned} S_t(X) &= \sum_{m,n<X} s(m+n)s(m-n)s(m)s(tn) \\ &= \sum_{m,n\leq\sqrt{X}} s(m^2-tn^2)s(m^2+tn^2) = \sum_{\substack{h\leq\sqrt{X}\\ h\in\mathcal{H}(t)}} \sum_{r\leq\sqrt{X}/h} 1 \\ &= \sum_{\substack{h\leq\sqrt{X}\\ h\in\mathcal{H}(t)}} \left\lfloor \frac{\sqrt{X}}{h} \right\rfloor = C_t X^{\frac{1}{2}} + O_t((\log X)^{r/2}). \end{aligned}$$

Proof Outline: From the construction of the arithmetic progression of squares from a right triangle, we have that $m^2 \pm tn^2$ are squares when $m \in H(t)$ and n relates to the area of the triangle so we see that

$$\begin{aligned} S_t(X) &= \sum_{m,n<X} s(m+n)s(m-n)s(m)s(tn) \\ &= \sum_{m,n\leq\sqrt{X}} s(m^2-tn^2)s(m^2+tn^2) = \sum_{\substack{h\leq\sqrt{X} \\ h\in\mathcal{H}(t)}} \sum_{r\leq\sqrt{X}/h} 1 \\ &= \sum_{\substack{h\leq\sqrt{X} \\ h\in\mathcal{H}(t)}} \left\lfloor \frac{\sqrt{X}}{h} \right\rfloor = C_t X^{\frac{1}{2}} + O_t((\log X)^{r/2}). \end{aligned}$$

We use the correspondence between rational right triangles and rational points on $E_t(\mathbb{Q})$, along with the known asymptotics of the number of rational points of bounded height, to get the asymptotic equivalence.

We note that $C_t \neq 0$, and equivalently $S_t(X)$ has polynomial growth in X, if and only t is a congruent number. Unfortunately, computing this series for large X by taking partial sums is no more efficient than running Euclid's ineffective algorithm and waiting for t to appear in it.

We note that $C_t \neq 0$, and equivalently $S_t(X)$ has polynomial growth in X, if and only t is a congruent number. Unfortunately, computing this series for large X by taking partial sums is no more efficient than running Euclid's ineffective algorithm and waiting for t to appear in it.

The hope is that taking inverse Mellin transforms of shifted multiple Dirichlet series of automorphic forms will afford us an alternate avenue for computing C_t directly.

Theta Functions

Let $\mathbb{H} \subset \mathbb{C}$ denote the **upper-half plane**, $\mathbb{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\}$.

Theta Functions

Let $\mathbb{H} \subset \mathbb{C}$ denote the **upper-half plane**, $\mathbb{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\}$.

Suppose for $z \in \mathbb{H}$ we define the **theta function**:

$$\theta(z) := \sum_{n \in \mathbb{Z}} e^{2\pi i n^2 z} = \sum_{n=0}^{\infty} r_1(n) e^{2\pi i n z} = 1 + 2\sum_{n=1}^{\infty} s(n) e^{2\pi i n z}$$

which is uniformly convergent on compact subsets of $\mathbb{H}$.

For $N \in \mathbb{N}$, let $\Gamma_0(N)$ denote the congruence subgroup:

$$\Gamma_0(N) := \left\{ \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix} \right) \in SL_2(\mathbb{Z}) \;\middle|\; N|C \right\}.$$

For $N \in \mathbb{N}$, let $\Gamma_0(N)$ denote the congruence subgroup:

$$\Gamma_0(N) := \left\{ \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \;\middle|\; N|C \right\}.$$

It is easy to show that $\Gamma_0(N)$ acts on $\mathbb{H}$ by Möbius Maps:

$$\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) z = \tfrac{Az+B}{Cz+D}.$$

For $N \in \mathbb{N}$, let $\Gamma_0(N)$ denote the congruence subgroup:

$$\Gamma_0(N) := \left\{ \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix} \right) \in SL_2(\mathbb{Z}) \;\middle|\; N|C \right\}.$$

It is easy to show that $\Gamma_0(N)$ acts on $\mathbb{H}$ by Möbius Maps:

$$\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix} \right) z = \tfrac{Az+B}{Cz+D}.$$

For $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix} \right) \in \Gamma_0(4)$, applying Poisson's summation formula on the generators of $\Gamma_0(4)$ allows us to prove that

$$\theta\left(\gamma z\right) = \left(\tfrac{C}{D}\right) \epsilon_D^{-1} \sqrt{Cz+D}\, \theta(z),$$

where $\left(\frac{C}{D}\right)$ denotes Shimura's extension of the Jacobi symbol and $\epsilon_D = 1$ or i depending on if $D \equiv 1$ or 3 (mod 4), respectively.[3]

For $N \in \mathbb{N}$, let $\Gamma_0(N)$ denote the congruence subgroup:

$$\Gamma_0(N) := \left\{ \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \;\middle|\; N|C \right\}.$$

It is easy to show that $\Gamma_0(N)$ acts on $\mathbb{H}$ by Möbius Maps:

$$\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) z = \tfrac{Az+B}{Cz+D}.$$

For $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_0(4)$, applying Poisson's summation formula on the generators of $\Gamma_0(4)$ allows us to prove that

$$\theta\left(\gamma z\right) = \left(\tfrac{C}{D}\right) \epsilon_D^{-1} \sqrt{Cz+D}\, \theta(z),$$

where $\left(\frac{C}{D}\right)$ denotes Shimura's extension of the Jacobi symbol and $\epsilon_D = 1$ or i depending on if $D \equiv 1$ or 3 (mod 4), respectively.[3]

We refer to $\theta(z)$ as a weight $1/2$ **holomorphic form** on $\Gamma_0(4)$.

To derive the asymptotics of $S_t(X)$, let Q be a large prime such that $Q > X$ and $(Q, t) = 1$, and let χ and ψ be characters mod Q.

To derive the asymptotics of $S_t(X)$, let Q be a large prime such that $Q > X$ and $(Q, t) = 1$, and let χ and ψ be characters mod Q.

Consider the shifted partial sums

$$S^{-}_{\chi,\psi}(X) := \sum_{m_1, n_1 < X} r_1(m_1 - n_1) r_1(m_1) \chi(m_1) \psi(n_1)$$

$$S^{+}_{\chi,\psi}(X; t) := \sum_{m_2, n_2 < X} r_1(m_2 + n_2) r_1(t n_2) \overline{\chi(m_2) \psi(n_2)}$$

To derive the asymptotics of $S_t(X)$, let Q be a large prime such that $Q > X$ and $(Q,t) = 1$, and let χ and ψ be characters mod Q.

Consider the shifted partial sums

$$S^{-}_{\chi,\psi}(X) := \sum_{m_1,n_1<X} r_1(m_1 - n_1) r_1(m_1) \chi(m_1) \psi(n_1)$$

$$S^{+}_{\chi,\psi}(X;t) := \sum_{m_2,n_2<X} r_1(m_2 + n_2) r_1(tn_2) \overline{\chi(m_2)\psi(n_2)}$$

Then the orthogonality properties for Dirichlet characters give us that

$$\sum_{\substack{\chi,\psi \\ (Q)}} S^{-}_{\chi,\psi}(X) S^{+}_{\chi,\psi}(X;t) = \sum_{m,n<X} r_1(m-n) r_1(m) r_1(m+n) r_1(tn).$$

The advantage of this approach is that we have some understanding how to drive asymptotic formulas for $S^{-}_{\chi,\psi}(X)$ and $S^{+}_{\chi,\psi}(X;t)$, at least modulo a thousand ugly details.

The advantage of this approach is that we have some understanding how to drive asymptotic formulas for $S^-_{\chi,\psi}(X)$ and $S^+_{\chi,\psi}(X;t)$, at least modulo a thousand ugly details.

Indeed, we can define the **twisted** theta function

$$\theta_\chi(z) = \sum_{m=0}^{\infty} r_1(m)\chi(m)e^{2\pi imz}$$

which, for $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_0(4Q^2)$, satisfies

$$\theta_\chi(\gamma z) = \chi^2(D)\left(\tfrac{C}{D}\right)\epsilon_D^{-1}\sqrt{Cz+D}\,\theta(z).$$

The advantage of this approach is that we have some understanding how to drive asymptotic formulas for $S^{-}_{\chi,\psi}(X)$ and $S^{+}_{\chi,\psi}(X;t)$, at least modulo a thousand ugly details.

Indeed, we can define the **twisted** theta function

$$\theta_\chi(z) = \sum_{m=0}^{\infty} r_1(m)\chi(m)e^{2\pi imz}$$

which, for $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_0(4Q^2)$, satisfies

$$\theta_\chi\left(\gamma z\right) = \chi^2(D)\left(\tfrac{C}{D}\right)\epsilon_D^{-1}\sqrt{Cz+D}\,\theta(z).$$

So we say $\theta_\chi(z)$ is a weight-$\frac{1}{2}$ holomorphic form of level $4Q^2$ and character χ^2.

Similarly, we observe that for square-free t,

Similarly, we observe that for square-free t,

$$\theta_\chi(tz) = \sum_{m=0}^{\infty} r_1(m)\chi(m)e^{2\pi i m t z} = \overline{\chi(n)} \sum_{m=0}^{\infty} r_1(tm)\chi(m)e^{2\pi i m z}$$

Similarly, we observe that for square-free t,

$$\theta_\chi(tz) = \sum_{m=0}^{\infty} r_1(m)\chi(m)e^{2\pi imtz} = \overline{\chi(n)} \sum_{m=0}^{\infty} r_1(tm)\chi(m)e^{2\pi imz}$$

and that for $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_0(4tQ^2)$ we have

$$\theta_\chi\left(t\gamma z\right) = \chi^2(D)\left(\tfrac{t}{D}\right)\left(\tfrac{C}{D}\right)\epsilon_D^{-1}\sqrt{Cz+D}\,\theta(tz).$$

Similarly, we observe that for square-free t,

$$\theta_\chi(tz) = \sum_{m=0}^{\infty} r_1(m)\chi(m)e^{2\pi imtz} = \overline{\chi(n)} \sum_{m=0}^{\infty} r_1(tm)\chi(m)e^{2\pi imz}$$

and that for $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_0(4tQ^2)$ we have

$$\theta_\chi(t\gamma z) = \chi^2(D)\left(\tfrac{t}{D}\right)\left(\tfrac{C}{D}\right)\epsilon_D^{-1}\sqrt{Cz+D}\,\theta(tz).$$

So we say $\theta_\chi(tz)$ is a weight-$\frac{1}{2}$ holomorphic form of level $4tQ^2$ and character $\left(\frac{t}{\cdot}\right)\chi^2$.

The take-away is that $r_1(m)$, $r_1(m)\chi(m)$ and $r_1(tn)\chi(n)$ are all the Fourier coefficients of holomorphic forms, and so we know how to get the meromorphic continuations of the shifted multiple Dirichlet series,

The take-away is that $r_1(m)$, $r_1(m)\chi(m)$ and $r_1(tn)\chi(n)$ are all the Fourier coefficients of holomorphic forms, and so we know how to get the meromorphic continuations of the shifted multiple Dirichlet series,

$$Z^{-}_{\chi,\psi}(s,w) := \sum_{m_1,n_1\geq 1} \frac{r_1(m_1-n_1)r_1(m_1)\chi(m_1)\psi(n_1)}{m_1^s n_1^w}$$

$$Z^{+}_{\chi,\psi}(s,w;t) := \sum_{m_2,h_2\geq 1} \frac{r_1(m_2+n_2)r_1(tn_2)\overline{\chi(m_2)\psi(n_2)}}{m_2^s n_2^w}$$

to all $(s,w)\in\mathbb{C}^2$ by using spectral expansions of Poincaré series.

The take-away is that $r_1(m)$, $r_1(m)\chi(m)$ and $r_1(tn)\chi(n)$ are all the Fourier coefficients of holomorphic forms, and so we know how to get the meromorphic continuations of the shifted multiple Dirichlet series,

$$Z^{-}_{\chi,\psi}(s,w) := \sum_{m_1,n_1\geq 1} \frac{r_1(m_1-n_1)r_1(m_1)\chi(m_1)\psi(n_1)}{m_1^s n_1^w}$$

$$Z^{+}_{\chi,\psi}(s,w;t) := \sum_{m_2,h_2\geq 1} \frac{r_1(m_2+n_2)r_1(tn_2)\overline{\chi(m_2)\psi(n_2)}}{m_2^s n_2^w}$$

to all $(s,w)\in\mathbb{C}^2$ by using spectral expansions of Poincaré series.

By taking inverse Mellin transforms of these objects, we are able to get the asymptotics of $S^{-}_{\chi,\psi}(X)$ and $S^{+}_{\chi,\psi}(X;t)$ and by averaging those over characters we may get the desired asymptotics of $S_t(X)$.

There are significant obstacles and potential downsides with this approach:

There are significant obstacles and potential downsides with this approach:

- As we take the limit with $Q \to \infty$, the level of the space we are taking the spectral expansion in qualitatively changes and so needs to be accounted for, especially in the continuous part of the spectrum. It is not obvious that this can be done in a completely general way for a given t.

There are significant obstacles and potential downsides with this approach:

- As we take the limit with $Q \to \infty$, the level of the space we are taking the spectral expansion in qualitatively changes and so needs to be accounted for, especially in the continuous part of the spectrum. It is not obvious that this can be done in a completely general way for a given t.

- It is not obvious that when this is done it will give us a coherent asymptotic formula for $S_t(X)$ or if the Q term will dominate and obscure the relevant asymptotic information.

There are significant obstacles and potential downsides with this approach:

- As we take the limit with $Q \to \infty$, the level of the space we are taking the spectral expansion in qualitatively changes and so needs to be accounted for, especially in the continuous part of the spectrum. It is not obvious that this can be done in a completely general way for a given t.

- It is not obvious that when this is done it will give us a coherent asymptotic formula for $S_t(X)$ or if the Q term will dominate and obscure the relevant asymptotic information.

- This approach could yield an asymptotic formula that is no better than the one we have already proven, and so not provide a reasonable alternative algorithm to checking if t is a congruent number.

The Congruent Number Zeta Function

Another approach might be to attempt to find a meromorphic continuation of the shifted multiple Dirichlet series:

The Congruent Number Zeta Function

Another approach might be to attempt to find a meromorphic continuation of the shifted multiple Dirichlet series:

$$Z_t(s) := \sum_{m,n=1}^{\infty} \frac{s(m-n)s(m)s(m+n)s(tn)}{m^s}.$$

As with $S_t(X)$, this series is nonzero exactly when square-free t is a congruent number.

The Congruent Number Zeta Function

Another approach might be to attempt to find a meromorphic continuation of the shifted multiple Dirichlet series:

$$Z_t(s) := \sum_{m,n=1}^{\infty} \frac{s(m-n)s(m)s(m+n)s(tn)}{m^s}.$$

As with $S_t(X)$, this series is nonzero exactly when square-free t is a congruent number.

From the reasoning in the proof of the asymptotic formula for $S_t(X)$, it is not difficult to show that

$$Z_t(S) = \zeta(2s) \sum_{h \in H(t)} \frac{1}{h^{2s}}$$

where, again, $\mathcal{H}(t)$, the set of hypotenuses, h, of dissimilar primitive right triangles with squarefree part of the area t.

So we can think of $L_t(s)$

$$Z_t(S) = \sum_{m,n=1}^{\infty} \frac{s(m-n)s(m)s(m+n)s(tn)}{m^s} = \zeta(2s) \sum_{h \in H(t)} \frac{1}{h^{2s}}$$

as a kind of congruent number zeta function and, as a corollary of our asymptotic formula:

So we can think of $L_t(s)$

$$Z_t(S) = \sum_{m,n=1}^{\infty} \frac{s(m-n)s(m)s(m+n)s(tn)}{m^s} = \zeta(2s) \sum_{h \in H(t)} \frac{1}{h^{2s}}$$

as a kind of congruent number zeta function and, as a corollary of our asymptotic formula:

$$S_t(X) := \sum_{m,n<X} s(m+n)s(m-n)s(m)s(tn) = C_t X^{\frac{1}{2}} + O_t((\log X)^{r/2}).$$

we see that $Z_t(s)$ that has continuation at least to $\Re(s) > 0$.

So we can think of $L_t(s)$

$$Z_t(S) = \sum_{m,n=1}^{\infty} \frac{s(m-n)s(m)s(m+n)s(tn)}{m^s} = \zeta(2s) \sum_{h \in H(t)} \frac{1}{h^{2s}}$$

as a kind of congruent number zeta function and, as a corollary of our asymptotic formula:

$$S_t(X) := \sum_{m,n<X} s(m+n)s(m-n)s(m)s(tn) = C_t X^{\frac{1}{2}} + O_t((\log X)^{r/2}).$$

we see that $Z_t(s)$ that has continuation at least to $\Re(s) > 0$.

The hope is that we can use spectral methods to represent $Z_t(s)$ in terms of spectral expansions and so bypass shifted sums altogether. It is also not obvious how whether this will work.

Thanks!

[1] L. E. Dickson.
History of the theory of numbers. Vol. II: Diophantine analysis.
Chelsea Publishing Co., New York, 1966.

[2] N. Koblitz.
Introduction to elliptic curves and modular forms, volume 97 of *Graduate Texts in Mathematics*.
Springer-Verlag, New York, second edition, 1993.

[3] G. Shimura.
On modular forms of half integral weight.
The Annals of Mathematics, 97(3):pp. 440–481, 1973.