Global Journal of Science Frontier Research: F
Mathematics & Decision Science
Volume 20 Issue 4 Version 1.0 Year 2020
Type : Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4626 & Print ISSN: 0975-5896

P = NP

By B. Litow

Abstract- We exhibit a polynomial time algorithm for the NP complete problem SBQR, size-bounded quadratic residues. This establishes the equality of the complexity classes P and NP. Proof of NP completeness was given in [3]. SBQR is the set of triples of the binary representations of the positive integers a; b; c such that there exists a positive integer x satisfying x2 _ a (mod b) and x _ c. W.L.O.G. we impose a, c $<$ b. Polynomial time means determinisic Turing machine time $\log^{O(1)} b$.

GJSFR-F Classification: *MSC 2010: 90C20 , 33E05*

PNP

Strictly as per the compliance and regulations of:

3. K. Manders and L. Adleman. NP-complete decision problems for binary quadratics. JCSS, 16:168–184, 1978.

P = NP

B. Litow

Abstract- We exhibit a polynomial time algorithm for the NP complete problem SBQR, size-bounded quadratic residues. This establishes the equality of the complexity classes P and NP. Proof of NP completeness was given in [3]. SBQR is the set of triples of the binary representations of the positive integers a, b, c such that there exists a positive integer x satisfying $x^2 \equiv a \pmod b$ and $x \leq c$. W.L.O.G. we impose $a, c < b$. Polynomial time means determinisic Turing machine time $\log^{O(1)} b$.

I. Introduction

We exhibit a polynomial time algorithm for the **NP** complete problem SBQR, size-bounded quadratic residues. This establishes the equality of the complexity classes **P** and **NP**. Proof of **NP** completeness was given in [3]. SBQR is the set of triples of the binary representations of the positive integers a, b, c such that there exists a positive integer x satisfying $x^2 \equiv a \pmod b$ and $x \leq c$. W.L.O.G. we impose $a, c < b$. Polynomial time means determinisic Turing machine time $\log^{O(1)} b$. We follow standard complexity class terminology [1].

II. A Sieve for SBQR

We reserve some notation.

- Unless otherwise indicated $O()$ notation indicates an absolute constant.
- $(x, y), [x, y]$, etc. denote real intervals, with a rounded bracket indicating the end-point is not included.
- $[x..y]$ is the set of integers z satisfying $x \leq z \leq y$.
- ℓ is the least integer satisfying $b^2 < 2^\ell$.
- $c_* = \lfloor (c^2 - a)/b \rfloor$. Note: $0 \leq c_* < b$.
- ι is the positive branch of $\sqrt{-1}$.
- $\tau = \iota/2^\ell + t$, where $t \in [0, 1]$ is a real variable. Note that any function of τ is obviously a function of t.
- $\mathbf{e}(z) = \exp(\pi \iota z)$. We regard π as represented by a rational but do not carry out the associated error analysis.
- $\Im(z)$ and $\Re(z)$ are the imaginary and real parts of complex z. Where brackets are unnecessary we will write $\Re z$ and $\Im z$.
- $T_{(m:f)}(z)$ is the sum of the first m terms of the Taylor series for $f(z)$.

Author: 6406 SE Tolman st. Portland OR 97206. e-mail: bruce.litow@gmail.com

We will frequently work with an integral of the form

$$g(t) = \int_u^v f(t,x)dx \ ,$$

where $t \in [0,1]$ and always $g(t)$ is continuous. This means that $\max_{t\in[0,1]} |g(t)|$ exists. Since $|g(t)| \leq \int_u^v |f(t,x)|dx$ an upper bound $O(\mu)$ on $\int_u^v |f(t,x)|dx$ is an upper bound on $\max_{t\in[0,1]} |g(t)|$. We will write $|g(t)| = O(\mu)$ rather than $\max_{t\in[0,1]} |g(t)| = O(\mu)$.

We define Ω to be

$$\int_0^1 \sum_{n=1}^{\infty} \mathbf{e}(n^2\tau) \cdot \sum_{j=1}^{c_*} \mathbf{e}(-(a+bj)t)dt \ . \tag{1}$$

The infinite summation exists because $\Im(\tau) > 0$.

The next lemma justifies calling Ω a sieve for SBQR.

Lemma 1 *If there exists a positive integer n satisfying $n \leq c$ and $n^2 \equiv a \pmod b$, then $\Omega > \exp(-\pi)$, else $\Omega = 0$.*

Proof: For integer k,

$$\int_0^1 \mathbf{e}(kt)dt = \begin{cases} 0 \text{ if } k \neq 0 \\ 1 \text{ if } k = 0 \end{cases} \tag{2}$$

Eq. 1 can be written as

$$\sum_{j=1}^{c_*} \sum_{n=1}^{\infty} \exp(-\pi n^2/2^\ell) \cdot \int_0^1 \mathbf{e}((n^2 - a - bj)t)dt \ . \tag{3}$$

All summands of Eq. 3 are nonnegative. The SBQR condition is equivalent to the existence of positive integers $n \leq c$ and $j \leq c_*$ such that $n^2 = a + bj$. The lemma follows from this equivalence, the value of ℓ, Eq. 2 and Eq. 3.

Our polynomial time algorithm for SBQR amounts to computing $\hat{\Omega}$ in polynomial time such that

$$|\Omega - \hat{\Omega}| < \exp(-\pi)/2 \ . \tag{4}$$

By Lemma 1 this solves SBQR in polynomial time.

III. Ω in Terms of a Theta Function

Define the Theta function $\vartheta(\tau)$ to be

$$1 + 2\sum_{n=1}^{\infty} (-1)^n \mathbf{e}(n^2\tau) \ . \tag{5}$$

From Eq. 5 we get

$$\sum_{n=1}^{\infty} (-1)^n \mathbf{e}(n^2\tau) = \frac{\vartheta(\tau) - 1}{2} \ . \tag{6}$$

Lemma 2 Ω *equals*

$$\sum_{j=1}^{c_*} \int_0^1 (-1)^{a+bj} \frac{\vartheta(\tau) - 1}{2} \mathbf{e}(-(a+bj)t) dt \ .$$

Proof: The expression for Ω matches Eq. 1 term by term except that each term of the infinite sum in Eq. 1 is multiplied by $(-1)^n(-1)^{a+bj}$. If $n^2 = a + bj$, then since $n \equiv n^2 \pmod 2$, $(-1)^n(-1)^{a+bj} = 1$. Terms with $n^2 \neq a+bj$ contribute 0 under integration so the sign of $(-1)^n(-1)^{a+bj}$ does not matter.

Lemma 2 suggests that the key to producing $\hat{\Omega}$ is a suitable polynomial time approximation of $\vartheta(\tau)$. Our approximation of $\vartheta(\tau)$ is based on

$$\vartheta(\tau) = -\iota \int_{\iota-\infty}^{\iota+\infty} \mathbf{e}(u^2\tau) \frac{1}{\sin(\pi u)} du \ . \tag{7}$$

A derivation of Eq. 7 due to R. Puzio [4] is included in section ?.

Before proceeding to approximate $\vartheta(\tau)$ we make an observation about a related Theta function, namely

$$\theta(\tau) = 1 + 2\sum_{n=1}^{\infty} \mathbf{e}(n^2\tau) \ ,$$

which is defined for $\Im\tau > 0$. Clearly, $\theta(\tau)$ is very similar to $\vartheta(\tau)$. Let γ be the matrix

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \ ,$$

where x, y, z, w are integers and $xw - yz = 1$. The action $\gamma \cdot \tau$ of γ on τ is defined by

$$\gamma \cdot \tau = \frac{x\tau + y}{z\tau + w} \ .$$

For given $t \in [1, 3]$ and corresponding τ there exists γ such that

$$\Im(\gamma \cdot \tau) \geq \sqrt{3}/2 \ .$$

Theorem 4.3 in Chap. III.4 [2] shows that if $z \equiv 0 \pmod 4$, then $\theta(\tau)$ can be expressed directly in terms of $\theta(\gamma \cdot \tau)$. Now, if $\Im(\gamma \cdot \tau) \geq \sqrt{3}/2$, then the series for $\theta(\gamma \cdot \tau)$ converges very rapidly and series truncation leads to very good approximation of $\theta(\tau)$. However, we do not know of an analogue of Eq. 7 for $\theta(\tau)$ and in our situation τ depends on t which ranges over $[0, 2]$. The choice of γ for which $\Im(\gamma \cdot \tau) \geq \sqrt{3}/2$ depends on the order of approximation of each value of t by rationals. The constraint $z \equiv 0 \pmod 4$ further complicates matters. These observations and Eq. 7 led us to work with $\vartheta(\tau)$.

IV. Approximating $\vartheta(\tau)$

The approximation of $\vartheta(\tau)$ will be carried out in three large steps. At some points in these steps additional results will be used: the recovery method and technical auxiliary lemmas. Proofs of the recovery method and auxiliary lemmas are in sections 5 and 6, respectively. Before proceeding we introduce some new parameters. For the rest of the paper the index j has range [0..3] and the index i has range [1..3]. We introduce four roots of unity: $\omega_0, \ldots, \omega_3$ as $1, \mathbf{e}(9/16), \mathbf{e}(2/3), \mathbf{e}(4/3)$, respectively.

Ref

2. N. Koblitz. Introduction to Elliptic Curves and Modular Forms. Springer, 1984.

Initial approximations will be carried out in Step 1. Much more detailed approximations are presented in Step 2. The final approximation of $\vartheta(\tau)$ is derived in Step 3 using the recovery method.

a) Step 1

Let $\kappa(t) = -\iota \exp(\pi/2^\ell) \exp(-t)$. Making the change of variable $x = u - \iota$ and noting $\tau = \iota/2^\ell + t$, Eq. 7 becomes

$$\kappa(t) \int_{-\infty}^{\infty} \frac{\exp(-\pi x^2/2^\ell)\mathbf{e}(x^2 t) \exp(-2\pi x t)\mathbf{e}(x/2^{\ell-1})}{\sin(\pi(x+\iota))} dx \ . \tag{8}$$

Define $B(t)$ to be

$$\kappa(t) \int_{-2^{\ell+4}}^{2^{\ell+4}} \frac{\exp(-\pi x^2/2^\ell)\mathbf{e}(x^2 t) \exp(-2\pi x t)\mathbf{e}(x/2^{\ell-1})}{\sin(\pi(x+\iota))} dx \ . \tag{9}$$

Lemma 3 $|\vartheta(\tau) - B(t)| = O(\exp(-2^\ell))$.

Proof: We will show that the sum of the absolute values of the integral of Eq. 8 over $(-\infty, -2^{\ell+4}]$ and $[2^{\ell+4}, \infty)$ is bounded above by $O(\exp(-2^\ell))$. We do this by bounding the absolute values of the integrand of Eq. 8 over these two half infinite ranges.

Now,

$$|\mathbf{e}(u^2\tau)| = |\exp(\pi/2^\ell) \exp(-\pi x^2/2^\ell) \exp(-2\pi x t)| \ .$$

Since $|\exp(\pi/2^\ell)| = O(1)$ it suffices to examine

$$|\exp(-\pi x^2/2^\ell) \exp(-2\pi x t)| \ . \tag{10}$$

The behavior of Eq. 10 depends on the behavior of $-\pi x^2/2^\ell - 2\pi x t$. By calculation, if $|x| \geq 2^{\ell+4}$, then $-\pi x^2/2^\ell - 2\pi x t \leq -|x|$. From this we see that if $|x| \geq 2^{\ell+4}$, then

$$|\mathbf{e}(u^2\tau)| = O(\exp(-|x|)) \ . \tag{11}$$

The lemma follows from Eq. 9, Eq. 11 and Eq. 64 of Lemma 8, section 6.

Define $B_+(t)$ to be

$$\kappa(t) \int_{0}^{2^{\ell+4}} \exp(-\pi x^2/2^\ell)\mathbf{e}(x^2 t) \exp(-2\pi x t)\mathbf{e}(x/2^{\ell-1}) \frac{1}{\sin(\pi(\iota+x))} dx$$

and $B_-(t)$ to be

$$\kappa(t) \int_{0}^{2^{\ell+4}} \exp(-\pi x^2/2^\ell)\mathbf{e}(x^2 t) \exp(2\pi x t)\mathbf{e}(-x/2^{\ell-1}) \frac{1}{\sin(\pi(\iota-x))} dx$$

Clearly, $B(t) = B_+(t) + B_-(t)$.

By Eq. 65 of Lemma 8 of section 6 we can express $B_+(t)$ as

$$-2\iota\kappa(t)\int_0^{2^{\ell+4}}\exp(-\pi x^2/2^\ell)\mathbf{e}(x^2t)\exp(-2\pi xt)\mathbf{e}(x/2^{\ell-1})\sum_{k=0}^{\infty}\exp(-2\pi k)\mathbf{e}(2(k+1)x)dx \tag{12}$$

and $B_-(t)$ as

$$-2\iota\kappa(t)\int_0^{2^{\ell+4}}\exp(-\pi x^2/2^\ell)\mathbf{e}(x^2t)\exp(2\pi xt)\mathbf{e}(-x/2^{\ell-1})\sum_{k=0}^{\infty}\exp(-2\pi k)\mathbf{e}(-2(k+1)x)dx\ . \tag{13}$$

$B_-(\omega_i t)$ is defined from Eq. 13 under the substitution $t \to \omega_i t$. Absorbing the -2ι factor redefine $\kappa(t) = -2\exp(\pi/2^\ell\mathbf{e}(-t)$.

Now we truncate the infinite sums in Eq. 12 and Eq. 13 to the first $\ell+1$ terms. Noting Eq. 12 define $B_{+,k}(t)$ to be

$$\kappa(t)\int_0^{2^{\ell+4}}\exp(-\pi x^2/2^\ell)\mathbf{e}(x^2t)\exp(-2\pi xt)\mathbf{e}(x/2^{\ell-1})\exp(-2\pi k)\mathbf{e}(2(k+1)x)dx \tag{14}$$

and noting Eq. 13 define $B_{-,k}(t)$ to be

$$\kappa(t)\int_0^{2^{\ell+4}}\exp(-\pi x^2/2^\ell)\mathbf{e}(x^2t)\exp(2\pi xt)\mathbf{e}(-x/2^{\ell-1})\exp(-2\pi k)\mathbf{e}(-2(k+1)x)dx\ . \tag{15}$$

$B_{-,k}(\omega_i t)$ is defined by Eq. 15 in the obvious way.

Now we introduce the truncated versions of $B_+(t), B_-(t)$ and $B_-(\omega_i t)$. Define $C_+(t)$ to be

$$\sum_{k=0}^{\ell}B_{+,k}(t) \tag{16}$$

and $C_-(t)$ to be

$$\sum_{k=0}^{\ell}B_{-,k}(t) \tag{17}$$

and $C_-(\omega_i t)$ to be

$$\sum_{k=0}^{\ell}B_{-,k}(\omega_i t) \tag{18}$$

A useful upper bound on the absolute value of the integrand of the integral defining $B_+(t)$ can be obtained but this does not apply to the integrand of the integral defining $B_-(t)$. It is possible to get useful bounds on the absolute value of the integrand of the integral defining $B_-(\omega_i t)$. Of course, $B_-(\omega_i t)$ is quite different to $B_-(t)$. We will use the recovery method of section 5 to overcome this difficulty.

Notes

The following definitions are of great importance.

- $\alpha_j = -\pi/2^\ell + \iota\pi t\omega_j$.
- $\beta_{0,k} = -2\pi t + \iota\pi(1/2^{\ell-1} + 2(k+1))$, where $k \in \mathbb{N}$.
- $\beta_{i,k} = 2\pi t\omega_i + \iota\pi(-1/2^{\ell-1} - 2(k+1))$, where $k \in \mathbb{N}$.

Using these definitions and Eq. 12 we can express $B_{+,k}(t)$ as

$$\kappa(t)\int_0^{\ell+4} \exp(-2\pi k)\exp(\alpha_0 x^2 + \beta_{0,k}x)dx \tag{19}$$

and using Eq. 13 we can express $B_{-,k}(\omega_i t)$ as

$$\kappa(t)\int_0^{\ell+4} \exp(-2\pi k)\exp(\alpha_i x^2 + \beta_{i,k}x)dx\ . \tag{20}$$

Lemma 4 $|\exp(\alpha_j x^2 + \beta_{j,k}x)| = O(1)$.

Proof: It suffices to show for $x \geq 0$ that

$$\Re(\alpha_j x^2 + \beta_{j,k}x) < 0\ .$$

This follows by inspection since $\Re(\alpha_j) < 0$ and $\Re(\beta_{j,k}) = 2\pi t\Re(2\pi t\omega_j) \leq 0$.

Note that

$$\Re(\beta_{i,k}) = 2\pi t\Re(2\pi t\omega_i) \leq 0$$

is the reason for introducing $\omega_1, \omega_2, \omega_3$. No satisfactory upper bound on

$$|\exp(\alpha_i x^2 + \beta_{i,k}x)|$$

exists if we set the ω_i to 1.

By Eq. 16, noting the factor $\exp(-2k\pi)$ in Eq. 19 and Lemma 4 we get

$$|B_+(t) - C_+(t)| = O(\ell 2^{\ell+4}\exp(-2\pi\ell)) \tag{21}$$

and similarly using Eq. 17 and Eq. 20,

$$|B_-(\omega_i t) - C_-(\omega_i t)| = O(\ell 2^{\ell+4}\exp(-2\pi\ell))\ . \tag{22}$$

b) Step 2

We break up the integration range $[0..2^{\ell+4}]$ into 'octaves', O_g. Let r be the least integer satisfying $\ell^2 < r$.

- $O_0 = [0, 2^r]$.
- for $g \in [1..\ell + 4 - r]$, $O_g = [2^{r+g-1}, 2^{r+g}]$.

Notes

From this point we reserve the symbols g and r. $O_{g,-}$ and $O_{g,+}$ denote the lower and upper endpoints of O_g. Integration restricted to $t \in O_g$ is denotes by $\int_{O_g}$. $B_{+,k,g}(t)$ is defined by Eq. 14 with integration restricted to $x \in O_g$ and $B_{-,k,g}(t)$ is defined by Eq. 15 with integration restricted to $x \in O_g$.

ith $x \in O_0$ we have by calculation

$$|\alpha_j x^2 + \beta_{j,k} x| = O(\ell^3) \ . \tag{23}$$

Define $D_{+,k,0}(t)$ to be

$$\int_{O_0} T_{(\ell^4:\exp)}(\alpha_0 x^2 + \beta_{0,k} x) dx$$

and define $D_{-,k,0}(\omega_i t)$ to be

$$\int_{O_0} T_{(\ell^4:\exp)}(\alpha_i x^2 + \beta_{i,k} x) dx$$

Using $O_0 = [0..2^r]$, the truncation error for the Taylor series for exp and Eq. 23 we get for $\ell > 2\exp(1)$ that

$$|D_{+,k,0}(t) - B_{+,k,0}(t| \text{ and } |D_{-,k,0}(\omega_i t) - B_{-,k,0}(\omega_i t| = O(\ell^2/2^{\ell^4}) \ . \tag{24}$$

Now, $x \in O_g$ for $g > 0$. Define $v_{j,k}$ to be

$$v_{j,k} = \alpha_j x^2 + \beta_{j,k} x \ . \tag{25}$$

Clearly,

$$|v_{j,k}| = O(2^{2\ell}) \ . \tag{26}$$

From Eq. 25 we get

$$dx = \frac{dv_{j,k}}{2\alpha_j x + \beta_{j,k}} \ . \tag{27}$$

We have, using $|\beta_{j,k}| = O(\ell)$ (reason for defining octaves):

$$1 \leq \frac{\max_{x \in O_g} |2\alpha_j x + \beta_{j,k}|}{\min_{x \in O_g} |2\alpha_j x + \beta_{j,k}|} = \frac{O_{g,+}}{O_{g,-}} \frac{1 \pm O(1/\ell)}{1 \pm O(1/\ell)} = 2 \pm O(1/\ell) < 3 \ . \tag{28}$$

Notice that the lower and upper bounds are independent of k. Using Eq. 28 and Lemma 9 of section 6, a polynomial $R_j(x)$ can be computed in polynomial time in m such that

$$|\frac{1}{2\alpha_j x + \beta_{j,k}} - R_j(x)| < 1/2^m \ . \tag{29}$$

Next, we want to express $R_j(x)$ by expressing x in terms of $v_{j,k}$. We do this by solving Eq. 25 for x. The solutions are

$$x = \frac{\beta_{j,k} \pm \sqrt{\beta_{j,k}^2 - 4\alpha_j v_{j,k}}}{2\alpha_j} \ .$$

By Eq. 25, at $x = 0$, $v_{j,k} = 0$ so we take the negative branch,

$$x = \frac{\beta_{j,k} - \sqrt{\beta_{j,k}^2 - 4\alpha_j v_{j,k}}}{2\alpha_j} \ . \tag{30}$$

Using Eq. 30 we can write $R_j(x)$ as

$$R_j(\frac{\beta_{j,k} - \sqrt{\beta_{j,k}^2 - 4\alpha_j v_{j,k}}}{2\alpha_j}) \ . \tag{31}$$

We can write Eq. 31 as

$$R_{j,1}(v_{j,k}) + R_{j,2}(v_{j,k}\sqrt{\beta_{j,k}^2 - 4\alpha_j v_{j,k}}) \ , \tag{32}$$

where $R_{1,j}(z)$ and $R_{j,2}(z)$ are polynomials.

Next, we approximate $\sqrt{\beta_{j,k}^2 - 4\alpha_j v_{j,k}}$ by a polynomial $R_{j,3}(v_{j,k})$. We first examine $\beta_{j,k}^2 - 4\alpha_j v_{j,k}$. Let $z_{j,k} = \beta_{j,k}^2 - 4\alpha_j v_{j,k}$. By inspection we get

$$|\frac{\Im(\iota z_{j,k})}{\Re(\iota z_{j,k})}| = O(1/\ell^2) \tag{33}$$

and

$$\frac{\max|\iota z_{j,k}|}{\min|\iota z_{j,k}|} = 4 \pm O(1/\ell^2) \ . \tag{34}$$

From the definition of $\beta_{j,k}$ one has

$$\Re(\iota z_{0,k}) < 0 \text{ and } \Re(\iota z_{i,k}) > 0 \ . \tag{35}$$

Let $\mu_j = \max_{x \in O_g} |z_{j,k}|$. Note that

$$|\mu_j| < 2^{O(\ell)} \ . \tag{36}$$

From Eq. 33, Eq. 34 and Eq. 35 one has

$$|\frac{\mu_0 + \iota z_{0,k}}{\mu_0}| = 3/4 \pm O(1/\ell^2) < 4/5 \text{ and } |\frac{\mu_i - \iota z_{i,k}}{\mu_i}| = 3/4 \pm O(1/\ell^2) < 4/5 \ . \tag{37}$$

Now,

$$\sqrt{\iota z_{0,k}} = \sqrt{\mu_0}\sqrt{1 - \frac{\mu_0 + \iota z_{0,k}}{\mu_0}}$$

and

$$\sqrt{\iota z_{i,k}} = \sqrt{\mu_i}\sqrt{1 - \frac{\mu_i - \iota z_{i,k}}{\mu_i}}$$

From these, Eq. 37 and the Taylor series for $\sqrt{1-\zeta}$ with

$$\zeta = 1 - \frac{\mu_0 + \iota z_{0,k}}{\mu_0}$$

and

$$\zeta = 1 - \frac{\mu_i - \iota z_{i,k}}{\mu_i}$$

we get

$$|\sqrt{\iota z_{0,k}} - \sqrt{\mu_0}(T_{(h:\sqrt{})}(\frac{\mu_0 + \iota z_{0,k}}{\mu_0}))| < \sqrt{\mu_0} \cdot (4/5)^h \tag{38}$$

and

$$|\sqrt{\iota z_{i,k}} - \sqrt{\mu_i}(T_{(h:\sqrt{})}(\frac{\mu_i - \iota z_{i,k}}{\mu_i}))| < \sqrt{\mu_i} \cdot (4/5)^h \ , \tag{39}$$

respectively.

By Eq. 36 if $h = 2\ell^2$ for ℓ sufficiently large the upper bounds in Eq. 38 and Eq. 39 can be replaced by $2^{-\ell^2}$. Eq. 38 and Eq. 39 extend to approximating $\sqrt{z_{j,k}}$ by using $\sqrt{\iota z_{j,k}} = \sqrt{\iota}\sqrt{z_{j,k}}$. Denote the resulting approximation polynomials as $P_0(v_{0,k})$ and $P_i(v_{i,k})$. By Eq. 39, a single polynomial works for all i but we retain the index so that we can write $P^j(v^{j,k})$ to cover all cases.

Recalling Eq. 32, define $R'_{j,k}(v_{j,k})$ to be

$$R_{j,2}(P_j(v_{j,k})) \ .$$

Using $h = 2\ell^2$ and the corresponding upper bound $2^{-\ell^2}$ in Eq. 38 and Eq. 39 and standard error estimations we obtain

$$|R_{j,2}(\sqrt{\beta_{j,k}^2 - 4\alpha_j v_{j,k}}) - R'_{j,k}(v_{j,k})| < 2^{-\ell^2/2} \ . \tag{40}$$

Recalling Eq. 31 define $Q_j(v_{j,k})$ to be

$$R_{j,1}(v_{j,k}) + R'_{j,k}(v_{j,k}) \tag{41}$$

With $j = 0$, $E_{+,k,g}(t)$ and with $j \in [1..3]$, $E_{-,k,g}(\omega_j t)$ is defined by

$$\int_{\tilde{O}_g} \exp(v_{j,k}) Q_j(v_{j,k}) dv_{j,k} \ , \tag{42}$$

where $\tilde{O}_g$ arises from O_g under the change of variable x to $v_{j,k}$.

Define $D_{+,k,g}(t)$ and $D_{-,k,g}(\omega_i t)$ by restricting the integrations to O_g in Eq. 19 and Eq. 20, respectively. Note that

$$D_{+,k}(t) = \sum_g D_{+,k,g}(t) \text{ and } D_{-,k}(\omega_i t) = \sum_g D_{-,k,g}(\omega_i t)$$

and similarly for $E_+(t)$ and $E_-(\omega_i t)$. From Lemma 4 and Eq. 42 we get

$$|E_{+,k,g}(t) - D_{+,k,g}(t)|, |E_{-,k,g}(\omega_i t) - D_{-,k,g}(\omega_i t)| < 2^{-2\ell} \ . \tag{43}$$

From the summations $\sum_k$ and $\sum_g$, the triangle inequality and Eq. 43 we get

$$|E_+(t) - D_+(t)| = O(\ell 2^{-2\ell}) \text{ and } |E_-(\omega_i t) - D_-(\omega_i t)| = O(\ell^2 2^{-2\ell}) \ . \tag{44}$$

By Lemma 10 the integration in Eq. 42 can be carried out exactly in polynomial time so that the evaluation of the integral in Eq. 42 can be expressed as

$$\exp(\gamma_{j,k,g,+}\omega_j t)U_{j,k,g,+}(\omega_j t) - \exp(\gamma_{j,k,g,-}\omega_j t)U_{k,g,-}(\omega_j t) \ , \tag{45}$$

where $\gamma_{j,k,g,+}$ and $\gamma_{j,k,g,-}$ are complex constants derived from $\tilde{O}_{g,+}$ and $\tilde{O}_{g,-}$, respectively and $U_{j,k,g,+}(\omega_j t)$ and $U_{k,g,-}(\omega_j t)$ are corresponding complex coefficient polynomials. For $j = 0$, Eq. 45 gives $E_{+,k,g}(t)$ explicitly and for $j \in [1..3]$ it gives $E_{-,k,g}(\omega_j t)$ explicitly.

Define

$$E_+(t) = \sum_k \sum_g E_{+.k,g}(t)$$

and

$$E_-(\omega_i t) = \sum_k \sum_g E_{-.k,g}(\omega_i t) \ .$$

c) Step 3

Via recovery, described in section 5 we will produce $E_-(t)$ from the $E_-(\omega_i t)$ and $\hat{\vartheta}(\tau) = E_+(t) + E_-(t)$ will be our approximation of $\vartheta(\tau)$. From Eq. 45, the comments immediately following, linearity of the recovery operator Υ and Eq. 63 of section 5 we can compute in polynomial time $E_-(t)$ given by

$$\Upsilon(E_{-,R}(\omega_1 t), E_{-,R}(\omega_2 t), E_{-,R}(\omega_3 t)) + \iota\Upsilon(E_{-,I}(\omega_1 t), E_{-,I}(\omega_2 t), E_{-,I}(\omega_3 t)) \ . E_{-,R}(\omega_i t) + \iota E_{-,I}(\omega_i t) \ . \tag{46}$$

It is clear that $\hat{\vartheta}(\tau)$ can be computed in polynomial time since $E_+(t)$ can be computed in polynomial time. Next, we determine an upper bound on $|\vartheta(\tau) - \hat{\vartheta}(\tau)|$.

Lemma 5 $|\vartheta(\tau) - \hat{\vartheta}(\tau)| = O(\ell^2 2^{-2\ell})$.

Proof: By Eq. 44,

$$|E_+(t) - D_+(t)| = O(\ell^2 2^{-2\ell}) \ . \tag{47}$$

By Eq. 21 and repeated triangle inequality using the fact that the summation range for k is $O(\ell)$,

$$|D_+(t) - C_+(t)| = O(\ell\delta) \ . \tag{48}$$

From Eq. 47 and Eq. 48,

$$|E_+(t) - C_+(t) = O(\ell^2 2^{-2\ell}) \ . \tag{49}$$

Again by Eq. 44,

$$|E_-(\omega_i t) - D_-(\omega_i t)| = O(\ell^2 2^{-2\ell}) \ . \tag{50}$$

By Eq. 22 and repeated triangle inequality using the fact that the summation range for k is $O(\ell)$,

$$|D_-(\omega_i t) - C_-(\omega_i t)| = O(\ell 2^{-2\ell}) \ . \tag{51}$$

From Eq. 50 and Eq. 51,

$$|E_-(\omega_i t) - C_-(\omega_i t)| = O(\ell^2 2^{-2\ell}) \ . \tag{52}$$

Notes

From Eq. 52, linearity of Υ and Lemma 7 of section 5,

$$|E_-(t) - C_-(t)| = O(\ell^2 2^{-2\ell}) \ .$$

Thus, we get, using $\hat{\vartheta}(\tau) = E_+(t) + E_-(t)$,

$$|\hat{\vartheta}(\tau) - (C_+(t) + C_-(t)| = O(\ell^2 2^{-2\ell}) \ .$$

Notes

The lemma follows from this, $B(t) = C_+(t) + C_-(t)$ and Lemma 3.

V. Computing $\hat{\Omega}$

Using $\hat{\vartheta}(\tau)$ we are ready to compute $\hat{\Omega}$ and verify Eq. 4. As observed in section 1, Eq. 4 and polynomial time computability of $\hat{\vartheta}(\tau)$ establishes that SBQR is in **P**.

Lemma 6

$$|\Omega - \hat{\Omega}| = O(\ell^2 2^{-\ell}) \ . \tag{53}$$

Proof: Noting Lemma. 2, define $\hat{\Omega}_* = \sum_{j=1}^{c_*} \hat{\Omega}_{*,j}$, where

$$\hat{\Omega}_{*,j} = \int_0^1 (-1)^{a+bj} \frac{\hat{\vartheta}(\tau) - 1}{2} \mathbf{e}(-(a+bj)t) dt \ . \tag{54}$$

By Lemma 5 and $|\mathbf{e}(-(a+bj)t)| = 1$,

$$|\int_0^1 (-1)^{a+bj} \frac{\vartheta(\tau) - 1}{2} \mathbf{e}(-(a+bj)t) dt - \hat{\Omega}_{*,j}| = O(\ell^2 2^{-2\ell}) \ . \tag{55}$$

By Eq. 45 $\hat{\Omega}_{*,j}$ can be exactly evaluated as an expression given by

$$\frac{(-1)^{a+bj} \exp(\zeta_+(a+bj))}{\zeta'_+(a+bj)^2} - \frac{(-1)^{a+bj} \exp(\zeta_-(a+bj))}{\zeta'_-(a+bj)^2} \ , \tag{56}$$

where ζ_+, ζ'_+ and ζ_-, ζ'_- are constants arising from evaluations at the integration endpoints 1 and 0, respectively. Clearly, Eq. 56 can be written as

$$\frac{\exp(\zeta''_+(a+bj))}{\zeta'_+(a+bj)^2} - \frac{\exp(\zeta''_-(a+bj))}{\zeta'_-(a+bj)^2} \ , \tag{57}$$

where $\zeta''_\pm = \zeta_\pm + \pi$.

Define $\hat{\Omega}$ to be

$$\sum_{j=1}^{c_*} \hat{\Omega}_{*,j} \ .$$

Lemma 11 of section 6 (adjusted for endpoints other than powers of 2), the summation range c_*, Eq. 55 and Eq. 57 give

$$|\Omega - \hat{\Omega}| = O(\ell^2 2^{-\ell}) \ ,$$

which is Eq. 53

For ℓ sufficiently large the bound $O(\ell^2 2^{-\ell})$ is less tha $\exp(-\pi)/2$, which satisfies Eq. 4.

VI. Recovery Method

We describe the recovery method. Let $f(t) = \sum_{n=0}^{\infty} f_n t^n$, where the f_n and t are real. Define $\sum_i$ to be

$$\sum_{n \equiv i \pmod 3} f_n t^n \ .$$

We have, using the reality of f_n,

$$\begin{aligned} f(\omega_1 t) &= \sum\nolimits_0 + \omega_1 \sum\nolimits_1 + \omega_1^2 \sum\nolimits_2 \\ f(\omega_2 t) &= \sum\nolimits_0 + \omega_2 \sum\nolimits_1 + \omega_3 \sum\nolimits_2 \\ f(\omega_3 t) &= \sum\nolimits_0 + \omega_3 \sum\nolimits_1 + \omega_2 \sum\nolimits_2 \end{aligned} \ . \tag{58}$$

Let $\mu_i = \Re(\omega_i)$ and $\nu_i = \Im(\omega_i)$ and $\mu_* = \Re(\omega_1^2)$. From Eq. 58 we get

$$\begin{aligned} \Re(f(\omega_1 t)) &= \sum\nolimits_0 + \mu_1 \sum\nolimits_1 + \mu_* \sum\nolimits_2 \\ \Im(f(\omega_2 t)) &= \nu_2 \sum\nolimits_1 + \nu_3 \sum\nolimits_2 \\ \Re(f(\omega_3 t)) &= \sum\nolimits_0 + \mu_3 \sum\nolimits_1 + \mu_2 \sum\nolimits_2 \end{aligned} \ . \tag{59}$$

Define X to be

$$\begin{pmatrix} 1 & \mu_1 & \mu_* \\ 0 & \nu_2 & \nu_3 \\ 1 & \mu_3 & \mu_2 \end{pmatrix} \ .$$

It is a calculation that

$$\mathrm{DET}(X) = -\sin(\pi/3)(2\cos(\pi/3) - \cos(9\pi/16) - \cos(9\pi/8)) \neq 0$$

so that X^{-1} exists. From Eq. 59 we get

$$\begin{pmatrix} \sum_0 \\ \sum_1 \\ \sum_2 \end{pmatrix} = X^{-1} \cdot \begin{pmatrix} \Re(f(\omega_1 t)) \\ \Im(f(\omega_2 t)) \\ \Re(f(\omega_3 t)) \end{pmatrix} \ . \tag{60}$$

We recover $f(t)$ through

$$f(t) = (1,1,1) \cdot X^{-1} \cdot \begin{pmatrix} \Re(f(\omega_1 t)) \\ \Im(f(\omega_2 t)) \\ \Re(f(\omega_3 t)) \end{pmatrix} \ . \tag{61}$$

For any 3×1 matrices u, v we have

$$(1,1,1) \cdot X^{-1} \cdot (u+v) = (1,1,1) \cdot X^{-1} \cdot u + (1,1,1) \cdot X^{-1} \cdot v \ . \tag{62}$$

We refer to $(1,1,1) \cdot X^{-1}$ as the recovery operator Υ and write its effect on the column vector of Eq. 61 as $\Upsilon(f(\omega_1 t)), (f(\omega_2 t)), (f(\omega_3 t)))$.

We give an extension to recovery and an error analysis. We need notation here. Let $g(z) = \sum_{n=0}^{\infty} g_n z^n$ where both the g_n and z may be complex. Define

$$g_R(z) = \sum_{n=0}^{\infty} \Re(g_n) z^n \text{ and } g_I(z) = \sum_{n=0}^{\infty} \Im(g_n) z^n \ .$$

Let t be real and let $f(t)$ have complex coefficients f_n. Given $f_R(\omega_1 t), f_R(\omega_2 t), f_R(\omega_3 t)$ and $f_I(\omega_1 t), f_I(\omega_2 t), f_I(\omega_3 t)$ it is clear that we can recover $f(t)$ as

$$f(t) = \Upsilon(f_R(\omega_1 t), f_R(\omega_2 t), f_R(\omega_3 t)) + \iota\Upsilon(f_I(\omega_1 t), f_I(\omega_2 t), f_I(\omega_3 t)) \ . \tag{63}$$

The decomposition $f(\omega_i t) = f_R(\omega_i t) + \iota f_I(\omega_i t)$ is always possible if $f(t)$ is given as a finite sum where the decomposition can be applied term by term and also holds for absolutely convergent infinite sums. This observation will apply to recovery applied to functions in this paper.

Notes

Lemma 7 *Assume t is real. If for $\omega \in \{\omega_1, \omega_2, \omega_3\}$, $|f(\omega t)| < \delta$, then $|f(t)| = O(\delta)$.*

Proof: For $\omega \in \{\omega_1, \omega_2, \omega_3\}$ assume $|f(\omega t)| < \delta$. Since $f(\omega t) = f_R(\omega t) + \iota f_I(\omega t)$ it follows that

$$|f_R(\omega t)| < \delta \text{ and } |f_I(\omega t)| < \delta \ .$$

From these inequalities, Eq. 62 and Eq. 63 we get

$$|f(t)| = |\Upsilon(f_R(\omega_1 t), f_R(\omega_2 t), f_R(\omega_3 t)) + \iota \cdot \Upsilon(f_I(\omega_1 t), f_I(\omega_2 t), f_I(\omega_3 t))| \leq O(\delta) \ .$$

Here the O notation reflects the $O(1)$ size of the entries of X^{-1}.

VII. Auxiliary Lemmas

Lemma 8 *For real x,*

$$\frac{1}{|\sin(\pi(\iota + x))|} = O(1) \tag{64}$$

and

$$\frac{1}{\sin(\pi(\iota + x))} = -2\iota \sum_{k=0}^{\infty} \exp(-2\pi k)\mathbf{e}(2(k+1)x) \ . \tag{65}$$

Proof: Let $z = \pi(1 - \iota x)$. Note that

$$\iota z = \pi(\iota + x).$$

Using

$$\exp(\iota \cdot \iota z) = \cos(\iota z) + \iota \sin(\iota z)$$

and

$$\exp(-\iota \cdot \iota z) = \cos(\iota z) - \iota \sin(\iota z)$$

we get

$$\sin(\pi(\iota + x)) = \frac{\exp(-z) - \exp(z)}{2\iota} \ .$$

Item 1 follows from this last equation.

It also follows that

$$\frac{1}{\sin(\pi(\iota + x))} = \frac{2\iota}{\exp(-z) - \exp(z)} \ . \tag{66}$$

The RHS of Eq. 66 can be written as

$$\frac{-2\iota \exp(-z)}{1-\exp(-2z)} .$$

Now

$$\exp(-2z) = \exp(-2\pi)\exp(2\pi\iota x) .$$

Thus, we can expand the RHS of Eq. 66 in geometric series as

$$-2\iota \sum_{k=0}^{\infty} \exp(-2\pi k)\exp(2(k+1)\pi\iota x) ,$$

which establishes item 2.

Lemma 9 *Assume* $0 < a < b$ *and* $a \leq |z|^2 \leq b$, *where* $z \in \mathbb{C}$.

$$|\frac{1}{z} - (\bar{z}/b)\sum_{k=0}^{h}((b-|z|^2)/b)^k| \leq (b/a)((b-\alpha)/b)^{h+1} ,$$

Proof:

$$\frac{1}{z} = \frac{\bar{z}}{|z|^2} = \frac{\bar{z}}{b-(b-|z|^2)} .$$

From this we get

$$\frac{1}{z} = (\bar{z}/b)\frac{1}{1-(b-|z|^2)/b} .$$

Now,

$$0 \leq (b-|z|^2)/b \leq (b-\alpha)/b < 1 .$$

From this and summing a geometric series, we get

$$|\frac{1}{z} - (\bar{z}/b)\sum_{k=0}^{h}((b-|z|^2)/b)^k| \leq (b/a)((b-\alpha)/b)^{h+1} ,$$

Lemma 9 assumes a simpler form when z is real.

Lemma 10 *If* γ *and* ν *are real and* $\sigma(t)$ *is either* $\cos(\nu t)$ *or* $\sin(\nu t)$, *then for* $h \in \mathbb{N}$,

$$U_h = \int_0^1 t^h \exp(\gamma t)\sigma(t)dt$$

can be computed in $h^{O(1)}$ *time. If* $\gamma = \nu = 0$ *this is trivial, otherwise* U_h *is a polynomial with general term*

$$\frac{Q_d(\gamma,\nu)}{(\gamma^2+\nu^2)^d} ,$$

where $d \in [0..h+1]$ *and* $Q_d(x,y)$ *is a bivariate polynomial.*

Proof: Proof is by straightforward integration by parts.

Lemma 11 *Assume $\sigma \geq 0$. Let $A = \sum_{f=2^p}^{2^q} \frac{1}{\sigma+f^2}$, where $0 \leq p < q$ are integers. A can be computed in polynomial time in terms of σ and q.*

Proof:

$$A = \sum_{j=0}^{q-p-1} \sum_{f=2^{p+j}}^{2^{p+j+1}-1} \frac{1}{\sigma + f^2} \, .$$

Next,

$$1 < \frac{\sigma + (2^{p+j+1}-1)^2}{\sigma + (2^{p+j})^2} < 4 \, .$$

By Lemma 9,

$$\sum_{f=2^{p+j}}^{2^{p+j+1}-1} \frac{1}{\sigma + f^2}$$

can be computed in polynomial time in terms of σ and q. The lemma follows since $j \in [0..q-p-1]$.

VIII. Derivation of Eq. 7

The following derivation of Eq. 7 is for a function denoted by $\vartheta_4(z|\tau)$. Our $\vartheta(\tau)$ is a special case of $\vartheta(z|\tau)$ with $z = 0$ and $\tau = 2t + \iota/2^\ell$. The identity is only needed in a compact domain of τ for our purpose.

The derivation begins by rearranging the Fourier series of $\cos(ux)$, one obtains the series

$$\frac{\pi \cos(ux)}{2u \sin(\pi u)} = \frac{1}{2u^2} + \sum_{n=1}^{\infty} (-1)^n \frac{\cos(nx)}{u^2 - n^2}$$

This equation which is valid for all real values of x such that $-\pi \leq x \leq \pi$ and all non-integral complex values of u. By comparison with the convergent series $\sum_{n=0}^{\infty} 1/n^2$, it follows that this series is absolutely convergent. Note that this series may be viewed as a Mittag-Leffler partial fraction expansion.

Let y be a positive real number. Multiply both sides by $2ue^{-yu^2}$ and integrate.

$$\int_{i-\infty}^{i+\infty} \frac{\pi \cos(ux) e^{-yu^2}}{\sin(\pi u)} \, dv = 2 \int_{i-\infty}^{i+\infty} e^{-yu^2} \left[\frac{1}{2u^2} + \sum_{n=0}^{\infty} (-1)^n \frac{\cos(nx)}{u^2 - n^2} \right] u \, du$$

Because of the exponential, the integrand decays rapidly as $u \to i \pm \infty$ provided that $\Re u > 0$, and hence the integral converges absolutely. Make a change of variables $v = u^2$

$$= \int_P e^{-yv} \left[\frac{1}{2v} + \sum_{n=1}^{\infty} (-1)^n \frac{\cos(nx)}{v - n^2} \right] dv$$

The contour of integration P is a parabola in the complex v-plane, symmetric about the real axis with vertex at $v = -1$, which encloses the real axis. Its equation is $\Re v + 1 = 2(\Im v)^2$

Let S_m (m is an integer) be the straight line segment joining the points $v = (i+m+1/2)^2$ and $v = (i-m-1/2)^2$. Along this line segment, we may bound the integrand in absolute value as follows:

$$\left|\sum_{n=1}^{\infty}(-1)^n\frac{\cos(nx)}{v-n^2}\right| \leq \sum_{n=1}^{\infty}\frac{(-1)^n}{|v-n^2|} \leq \sum_{n=1}^{\infty}\frac{(-1)^n}{|v_m-n^2|}$$

where $v_m = m^2+m-3/4$ is the point of intersection of S_m with the real axis. To proceed further, we break up the last summation into two parts.

Since the squares closest in absolute value to v_m are m^2 and $(m+1)^2 = m^2+2m+1$, it follows that $|v_m - n^2| \geq |m-3/4|$ for all m, n. Hence, we have

$$\sum_{i=1}^{2m}\frac{1}{|v_m-n^2|} \leq \frac{2m}{m-3/4} \leq 8$$

When $n > 2m$, we have $n^2 \geq (2m+1)^2 = 4m^2+4m+1 > 4m^2+4m-3 = 4v_m$. Hence, $|n^2 - v_m| > 3n^2/4$ and

$$\sum_{n=2m+1}^{\infty}\frac{1}{|v_m-n^2|} < \frac{4}{3}\sum_{n=2m+1}^{\infty}\frac{1}{n^2} < \frac{4}{3}\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{2\pi}{9}$$

Finally $1/(2v_m) < 1/2$ since $v_m > 1$ when $m \geq 1$. Also, $|e^{-yv}| = e^{-y\Re v} - e^{-yv_m} < e^{-ym^2}$. From these observations, we conclude that

$$\left|\int_{S_m} e^{-yv}\left[\frac{1}{2v}+\sum_{n=1}^{\infty}(-1)^n\frac{\cos(nx)}{v-n^2}\right]dv\right| < e^{-ym^2}\left(1+8+\frac{2\pi}{9}\right)\int_{S_m}dv = (4m+2)\left(9+\frac{2\pi}{9}\right)e^{-ym^2}$$

Note that this quantity approaches 0 in the limit $m \to \infty$.

Let P_m be the arc of the parabola P bounded by the endpoints of S_m. Together, S_m and P_m form a closed contour which encloses poles of the integrand. Hence, by the residue theorem , we have

$$\int_{P_m} e^{-yv}\left[\frac{1}{2v}+\sum_{n=1}^{\infty}(-1)^n\frac{\cos(nx)}{v-n^2}\right]dv + \int_{S_m} e^{-yv}\left[\frac{1}{2v}+\sum_{n=1}^{\infty}(-1)^n\frac{\cos(nx)}{v-n^2}\right]dv =$$

$$2\pi i\sum_{n=1}^{m}(-1)^n\cos(nx)e^{-n^2y}$$

Taking the limit $m \to \infty$ we obtain

$$\int_{P} e^{-yv}\left[\frac{1}{2v}+\sum_{n=1}^{\infty}(-1)^n\frac{\cos(nx)}{v-n^2}\right]dv = 2\pi i\left(\frac{1}{2}+\sum_{n=1}^{\infty}(-1)^n\cos(nx)e^{-n^2y}\right)$$

Going back to the beginning of the proof, where the integral on the left hand side was expressed as an integral with respect to u, we obtain

$$\int_{i-\infty}^{i+\infty}\frac{\pi\cos(ux)e^{-yu^2}}{\sin(\pi u)}dv = 2\pi i\left(\frac{1}{2}+\sum_{n=1}^{\infty}(-1)^n\cos(nx)e^{-n^2y}\right)$$

Making a change of variables $x = 2z, y = -i\pi\tau$ and tidying up some, we obtain

$$\int_{i-\infty}^{i+\infty}\frac{\cos(2uz)e^{i\pi\tau u^2}}{\sin(\pi u)}dv = i\left(1+2\sum_{n=1}^{\infty}(-1)^n e^{i\pi n^2\tau}\cos(2nz)\right) = i\vartheta_4(z|\tau)$$

Because of the initial assumption about the Fourier series, we only know that this formula is valid when τ is purely imaginary with strictly positive imaginary part and z is real and $\pi/2 < z < \pi/2$. However, we can use analytic continuation to extend the domain of its validity. On the one hand, the theta function on the right-hand side is analytic for all z and all τ such that $\Im\tau > 0$.

On the other hand, I claim that the integral on the left hand side is also an analytic function of z and τ whenever $\Im\tau > 0$. To validate this claim, we need to examine the behaviour of the integrand as $u \to i\pm\infty$. The contribution of the denominator is bounded;

$$\left|\frac{1}{\sin \pi u}\right| < c$$

for some constant c whenever $\Im u = 1$. The absolute value of the cosine in the numerator is easy to bound:

$$|\cos(2uz)| \leq e^{2|u|\,|z|}$$

To bound the remaining term, let us examine the argument of the exponential carefully:

$$\Im(\tau u^2) = 2\Re\tau\,\Re u + \Im\tau(\Re u)^2 - \Im\tau = \Im\tau\left(\left(\Re u + \frac{\Re\tau}{\Im\tau}\right)^2 - 1 - \left(\frac{\Re\tau}{\Im\tau}\right)^2\right)$$

Therefore, if $|\Re u| > 1 + 3|\Re\tau|/(\Im\tau)$, it will be the case that $\Im(\tau u^2) \geq \Im\tau\,(\Re u)^2/9$, and so

$$\left|e^{i\pi\tau u^2}\right| = e^{-\pi\Im(\tau u^2)} \leq e^{-\pi\Im\tau\,(\Re u)^2/9}$$

Taken together, the estimates of the last paragraph imply that

$$\left|\int_{i+R}^{i+\infty} \frac{\cos(2uz)e^{i\pi\tau u^2}}{\sin(\pi u)}\right| < c\int_{i+R}^{i+\infty} e^{2|u||z|-\pi\Im\tau\,(\Re u)^2/9}$$

when $R > 1 + 3|\Re\tau|/(\Im\tau)$. If we impose the further conditions

$$R > \frac{180|z|}{\pi\,\Im\tau} \qquad R^2 > \frac{180|z|}{\pi\,\Im\tau}\ ,$$

it will be the case that

$$2|u||z| - \pi\Im\tau\,(\Re u)^2/9 < 2\Re u\,|z| + 2|z| - \pi\Im\tau\,(\Re u)^2/9 <$$
$$\left(2\Re u\,|z| - \pi\Im\tau\,(\Re u)^2/180\right) + \left(2|z| - \pi\Im\tau\,(\Re u)^2/180\right) - \pi\Im\tau\,(\Re u)^2/10 <$$
$$-\pi\Im\tau\,(\Re u)^2/10\,,$$

and hence

$$\left|\int_{i+R}^{i+\infty} \frac{\cos(2uz)e^{i\pi\tau u^2}}{\sin(\pi u)}\,du\right| < c\int_{i+R}^{i+\infty} e^{-\pi\Im\tau\,(\Re u)^2/10}\,du < \frac{5c}{\pi\,\Im\tau}Re^{-\pi\Im\tau\,R^2/10}.$$

Likewise, under the same restriction on R,

$$\left|\int_{i-\infty}^{i-R} \frac{\cos(2uz)e^{i\pi\tau u^2}}{\sin(\pi u)}\,du\right| < c\int_{i+R}^{i+\infty} e^{-\pi\Im\tau\,(\Re u)^2/10}\,du < \frac{5c}{\pi\,\Im\tau}Re^{-\pi\Im\tau\,R^2/10}.$$

Since the contour of integration is compact and the integrand is analytic in a neighborhood of the contour,

$$\int_{i-R}^{i+R} \frac{\cos(2uz)e^{i\pi\tau u^2}}{\sin(\pi u)}\,du$$

will be an analytic function of z and τ. Suppose that z and τ are restricted to bounded regions of the complex plane and that, furthermore, $Im\tau$ is positive and bounded away from zero. Then the inequalities of the last paragraph imply that the integral converges uniformly as $R \to \infty$, and hence

$$\int_{i-\infty}^{i+\infty} \frac{\cos(2uz)e^{i\pi\tau u^2}}{\sin(\pi u)}\,du$$

is an analytic function of u and z in the domain $\Im\tau > 0$.

Thus, by the fundamental theorem of analytic continuation, we may conclude that

$$\int_{i-\infty}^{i+\infty} \frac{\cos(2uz)e^{i\pi\tau u^2}}{\sin(\pi u)}\,dv = i\left(1 + 2\sum_{n=1}^{\infty}(-1)^n e^{i\pi n^2\tau}\cos(2nz)\right) = i\vartheta_4(z|\tau)$$

throughout this domain.

References Références Referencias

1. T. Cormen, C. Leiserson, R. Rivest, and C. Stein. Introduction to Algorithms. MIT, 2009, 3rd ed.
2. N. Koblitz. Introduction to Elliptic Curves and Modular Forms. Springer, 1984.
3. K. Manders and L. Adleman. NP-complete decision problems for binary quadratics. JCSS, 16:168–184, 1978.
4. planet math CC-BY-SA 3.0. integral form of Theta. http://planetmath.org/derivationofintegralrepresentationsofjacobivarthetafunctions, 2013, 03/21.

Notes