Hecke eigenfunctions of quantized cat maps modulo prime powers

Rikard Olofsson *

April 17, 2009

Abstract

This paper continues the work done in [16] about the supremum norm of eigenfunctions of desymmetrized quantized cat maps. N will denote the inverse of Planck's constant and we will see that the arithmetic properties of N play an important role. We prove the sharp estimate $\|\psi\|_\infty = O(N^{1/4})$ for all normalized eigenfunctions and all N outside of a small exceptional set. We are also able to calculate the value of the supremum norms for most of the so called newforms. For a given $N = p^n$, with $n > 1$, the newforms can be divided in two parts (leaving out a small number of them in some cases), the first half all have supremum norm about $2/\sqrt{1 \pm 1/p}$ and the supremum norm of the newforms in the second half have at most three different values, all of the order $N^{1/6}$. The only dependence of A is that the normalization factor is different if A has eigenvectors modulo p or not. We also calculate the joint value distribution of the absolute value of n different newforms.

1 Introduction

This paper studies one of the simplest, and perhaps most popular, models in quantum chaos, the so called quantized cat map. It is the quantization of the discrete time chaotic dynamical system where in each time step the point $x \in \mathbb{T}^2 = \mathbb{R}^2/\mathbb{Z}^2$ is mapped to $Ax \in \mathbb{T}^2$ for some given hyperbolic (i.e. with $|\operatorname{tr}(A)| > 2$) matrix $A \in SL(2,\mathbb{Z})$. The dynamics is quantized through a unitary operator $U_N(A)$ (called the quantum propagator) acting on $L^2(\mathbb{Z}_N) = L^2(\mathbb{Z}/N\mathbb{Z})$, which is referred to as the state space. This space is of course isomorphic to $\mathbb{C}^N$ and the interest lies mostly within studying the properties of the eigenfunctions of $U_N(A)$ as the dimension N of the state space grows to infinity. The limit as N goes to infinity is called the semiclassical limit and N^{-1} can be interpreted as Planck's constant. One hopes to find properties that correspond to the fact that the classical system is ergodic. It is for instance natural to study the measures the eigenfunctions induce on the torus and see if they get close to the Lebesgue measure in the limit. It is well known that Schnirelman's theorem holds for the cat map, or in other words, that the cat map is quantum ergodic [4, 19].

*Department of Mathematics, KTH, SE-100 44 Stockholm, Sweden *E-mail address*: rikardo@math.kth.se The author is supported by grant KAW 2005.0098 from the Knut and Alice Wallenberg Foundation.

This means that the induced limit of most eigenfunctions converge weakly to the Lebesgue measure. More formally the statement can be written as follows: Given a triangle of eigenfunctions $\psi_{N,j} \in L^2(\mathbb{Z}/NZ)$, where $j = 1, 2, ..., N$ and $N = 1, 2, 3, ...$ there exist sets $E(N) \subseteq \{1, ..., N\}$ satisfying

$$\lim_{N \to \infty} \frac{\#E(N)}{N} = 1$$

such that for all functions $f \in C^\infty(\mathbb{T}^2)$ and all maps $j : N \in \mathbb{N} \mapsto j(N) \in E(N)$ we have

$$\lim_{N \to \infty} \langle Op_N(f)\psi_{N,j(N)}, \psi_{N,j(N)}\rangle = \int_{\mathbb{T}^2} f(x)dx.$$

The obvious question is if we can replace "most eigenfunctions" with "all eigenfunction", i.e., whether we can take $E(N) = \{1, 2, 3, ..., N\}$ in the statement above or not. This is the question of quantum unique ergodicity (QUE). It was proven by Faure, Nonnenmacher and De Biévre that the cat map is not quantum unique ergodic [7]. Given any periodic orbit of the dynamics (for instance the origin), they were able to construct sequences of induced measures which converge to 1/2 times Lebesgue measure plus 1/2 times normalized Dirac measure of the orbit. The phenomenon when induced measures concentrate on periodic orbits is called scarring and the result shows that this can occur.

The reason that the quantum unique ergodicity fails is that for some N the order of A modulo N is extremely small. Small order leads to large dimensions of the eigenspaces of $U_N(A)$ and that means a good possibility to find a bad eigenfunction. To cope with this problem, Kurlberg and Rudnick viewed $U_N(A)$ as an element in a group of commuting operators and studied their joint eigenfunctions. In this way they desymmetrized the problem and made the dimensions of the studied subspaces small. In analogy with the theory of modular forms they called the elements in the group Hecke operators and the common eigenfunctions Hecke eigenfunctions. Kurlberg and Rudnick showed that the induced measures of Hecke eigenfunctions converges weakly to Lebesgue measure, i.e., that the desymmetrized model is quantum unique ergodic [13].

Instead of studying the induced limits this paper is devoted to studying the supremum norm of the eigenfunctions. This question has received a lot of attention in quantum chaos, for instance in [8, 1, 9, 17, 2, 3], but in this introduction we will try to focus on the results for the quantized cat map. To understand these results two properties of $U_N(A)$ are important to know: First of all, if $N = p_1^{n_1} p_2^{n_2} ... p_r^{n_r}$ we can define $U_N(A)$ as the tensor product of $U_{p_j^{n_j}}(A)$ for $j = 1, ..., r$. Thus we may restrict ourselves to the case $N = p^n$, where p is a prime. Secondly, for $N = p^n$ we will define $U_N(A)$ so that it gives a representation of $SL(2, \mathbb{Z}_N)$. This enables us to define the Hecke eigenfunctions as elements in the representations corresponding to a specific character when U_N is restricted to some abelian subgroup of $SL(2, \mathbb{Z}_N)$ which contains the image of A in $SL(2, \mathbb{Z}_N)$.

In [16] it was observed that there are large differences between the case $n = 1$ and all other possible values of n. One of the reasons for this is the existence of invariant subspaces of $L^2(\mathbb{Z}_N)$ such that the functions in these subspaces have their support on ideals of $\mathbb{Z}_N$. These representations are isomorphic to $U_{N'}$ for some $N'|N$ and this isomorphism is easy to write down. We will call the Hecke eigenfunctions belonging to any of these subspaces oldforms, in analogy with the

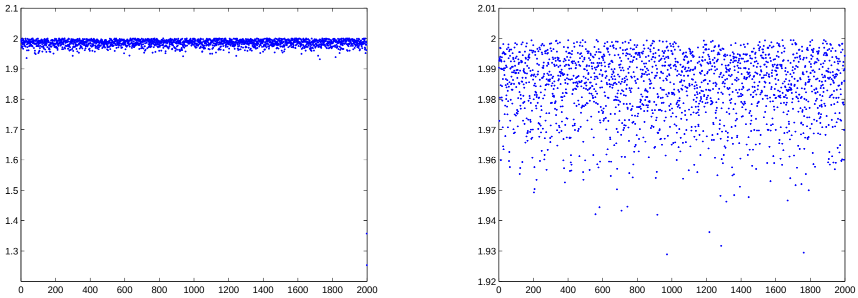

Figure 1: The supremum norm of all Hecke eigenfunctions of two different matrices A. Both pictures are for the prime $N = 1999$, but in the left picture A makes N split and in the right picture A makes N inert. There exists an element in the Hecke group such that the corresponding eigenvalues, when evaluated at this element, are listed with growing phase in the interval $(-\pi, \pi]$.

theory of modular forms. The Hecke eigenfunctions orthogonal to the oldforms are called newforms. We will give an exact definition of oldforms and restate the theorem mentioned above in Chapter 3.

Another large difference observed in [16] is that when $N = p^n$ and $n > 1$ the supremum norm of newforms have very distinct values (compare Figure 1 with Figure 2). These values were calculated in the case when n was even. When N is a prime we do not have this behavior. The main interest of this paper is to generalize the ideas of [16] in order to prove the observation and calculate the supremum norms also in the case when $N = p^n$ and $n \geqslant 3$ is odd. We will see that the results are very similar to the results obtained in [16]. More precisely we will show that given a matrix A and a prime power N an arithmetic condition will split the set of newforms in two parts of the same size, leaving out a small number of newforms. In the first part all the newforms have supremum norm in a very small interval just below $2/\sqrt{1 \pm 1/p}$, where the sign depends on if A has eigenvectors or not modulo p. The newforms in the second part have much larger supremum norms, all about $N^{1/6}$. If $n \equiv 0 \pmod 3$ or if $p \equiv 2 \pmod 3$ all newforms in this part have exactly the same supremum norm and otherwise the supremum norms assumes at most 3 different values. Note that we need to desymmetrize to get our results, since obviously the subspaces need to be one dimensional if we want to calculate the supremum norm of its normalized elements.

As a consequence of our formulas for the supremum norm of newforms we get estimates on the supremum norm of general Hecke eigenfunctions. The best result for the supremum norm of Hecke eigenfunctions for a general N was obtained by Kurlberg and Rudnick in [14]. They prove that for a fixed hyperbolic matrix A, the supremum norm of a L^2-normalized Hecke eigenfunction is bounded by $O(N^{3/8+\epsilon})$. Once again this is in great contrast to the estimates one can get if N is a prime because then one can do much, much better. If N is a prime, the supremum norm is bounded by $2/\sqrt{1 \pm 1/N}$, where the sign is the same as in prime power case above [14, 12]. In Figure 1 we can see that these

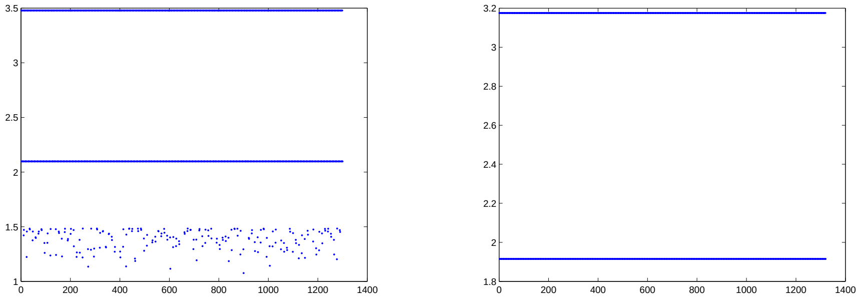

Figure 2: Here $N = 11^3$ and we only print the supremum norms of newforms. The left picture is when 11 is split while the right picture is when 11 is inert. The ordering is the same as above.

bounds are essentially sharp. As a consequence of these good bounds the tensor decomposition tells us that if N is square free the supremum norm is bounded by $O(N^{\epsilon})$ [12]. However, the square free case is special because in [16] I showed that for $N = a^2b$ there exists a Hecke eigenfunction such that its supremum norm is at least $a^{1/2}$. In particular if $N = a^2$ we have an oldform with supremum norm $N^{1/4}$. The theorem below tells us that this is the maximal value, i.e. we show that the supremum norm is always $O(N^{1/4})$. These estimates are not for a general N, but almost. Fixing a hyperbolic matrix A we throw away a finite number of "bad primes"; the first "bad prime" is 2, then all primes such that A is upper triangular modulo p are "bad" and finally the primes such that $p| \operatorname{tr}(A)^2 - 4$ are "bad". This is obviously a finite set of primes since A is not upper triangular itself. Now choose a positive integer m. We say that N is good with respect to m if no "bad prime" p is such that $p^m|N$. It is easy to see that the proportion of integers which are good tends to 1 as we let m grow. Our theorem can now be stated as follows:

Theorem 1.1. *Fix a hyperbolic matrix $A \in SL(2, \mathbb{Z})$ and an integer $m \in \mathbb{Z}_+$. If N is good with respect to m and $\psi \in L^2(\mathbb{Z}_N)$ is a L^2-normalized Hecke eigenfunction, then*

$$\|\psi\|_\infty = O_m(N^{1/4}).$$

Remark. The reason we do not study the exponents of "bad primes" is mostly technical. I have no reason to suspect that the estimate should not hold for any N, other than that calculations become much more difficult for "bad primes".

Let us turn to the question of value distribution of the Hecke eigenfunctions. We will let $N = p^n$, where $n > 1$ is fixed and let p grow to infinity. In [14] Kurlberg and Rudnick studied the same problem, but for $n = 1$ and A diagonalizable modulo p. They showed that the value distribution of the absolute values converge to a semi-circle measure on the interval $[0, 2]$ and that the convergence of the values of different eigenfunctions are statistically independent. The semi-circle measure can be interpreted as the image of Haar measure of $SU(2)$ under the map $g \mapsto |\operatorname{tr}(g)|$. They went on in [15] to conjecture that the fluctuations of the normalized matrix elements converge, as N go to infinity through the primes, to random variables given by sums of independent random variables with the measure given by the image of Haar measure of $SU(2)$ under the map $g \mapsto \operatorname{tr}(g)$. In [10] Kelmer showed that for $N = p^n$, with $n > 1$ fixed, the fluctuations do indeed converge to a sum of independent random variables in the conjectured manner. The distribution of the random variables in this case is however not the same as when N is prime, instead the distribution is given by the image of the Haar measure of the normalizer of the maximal torus of $SU(2)$ under the map $g \mapsto \operatorname{tr}(g)$. With this result in mind and the conjecture of Kurlberg and Rudnick it seems like a good guess to hope to show that the value distribution of the absolute value of newforms converge to the image of Haar measure of the normalizer of the maximal torus under the map $g \mapsto |\operatorname{tr}(g)|$. This is also precisely our result. We also show that if d newforms are chosen from different subspaces (to be specified later) their absolute values are statistically independent. The exact statement is the following:

Theorem 1.2. *Fix $n > 1$ and let p grow through the primes. Let f be a continuous bounded function on $\mathbb{R}^d$ and let $\psi_{p,j} \in V_{C_j}$ for some $C_j \in \mathbb{Z}^{\times}_{p^{[n/2]}}$ where $j = 1, 2, ..., d$ be d sequences of normalized newforms. Assume also that $C_i \not\equiv C_j \pmod{p}$ for $i \neq j$. Then*

$$\lim_{p\to\infty} \frac{1}{p^n} \sum_{x\in\mathbb{Z}_{p^n}} f(|\psi_{p,1}(x)|, |\psi_{p,2}(x)|, ..., |\psi_{p,d}(x)|) = \int_{\mathbb{R}^d} f(y) d\mu^d(y).$$

Remark. The measure μ is written down explicitly in Equation 13 and the spaces V_C are defined in Definition 3.7 for n odd and Definition 5.5 in [16] for even n.

Theorem 1.2 says that the distribution of the absolute value of "generic" newforms will converge to the limiting measure and that this convergence is statistically independent if the C_j are different modulo p.

Making only small corrections to the proof of Theorem 1.2 one can also evaluate autocorrelation functions by showing that the absolute value of ψ at different points ("generically chosen") is also statistically independent. In other words, one can easily obtain:

Theorem 1.3. *Fix $n > 1$ and let p grow through the primes. Let f be a continuous bounded function on $\mathbb{R}^d$ and let $\psi_p \in V_C$ for some $C \in \mathbb{Z}^{\times}_{p^{[n/2]}}$ be a sequence of normalized newforms. Let $x_{p,j}$, where $j = 1, 2, ..., d$ be d sequences of points $x_{p,j} \in \mathbb{Z}_{p^n}$ such that $x_{p,i} \not\equiv x_{p,j} \pmod{p}$ for $i \neq j$. Then*

$$\lim_{p\to\infty} \frac{1}{p^n} \sum_{x\in\mathbb{Z}_{p^n}} f(|\psi_p(x+x_{p,1})|, |\psi_p(x+x_{p,2})|, ..., |\psi_p(x+x_{p,d})|) = \int_{\mathbb{R}^d} f(y) d\mu^d(y).$$

Remark. We will only prove Theorem 1.2 and leave the corrections in order to prove Theorem 1.3 to the reader.

Note that there is no interest in studying also the oldforms, since their value distribution trivially converges to zero. We also remark that our value distribution (in contrast to the semi-circle measure) shows a large probability to be close to 2 (see the beginning of Chapter 1.2 for a more explicit formula for the value distribution) and this explains why we obtain our lowest line in Figure 2 and why we do not see this line in Figure 1.

Since the entropy of quantum states has received so much recent attention it seems appropriate to observe that the value distribution gives us the asymptotic behavior of the Shannon entropy of the newforms. We see that the entropy is maximal, i.e., the following corollary holds:

Corollary 1.4. *The Shannon entropy of any sequence ψ_N of normalized newforms fulfills*

$$\lim_{N\to\infty}\frac{h(\psi)}{\log N}=1.$$

This is in great contrast to the entropy of oldforms, which can be as small as $1/2\log N$.

2 Acknowledgments

I would like to thank Pär Kurlberg for his help and encouragement. I also thank Carel Faber for the helpful discussions we have had.

3 Basic definitions and concepts

The dynamical system we will quantize can be described as a matrix $A\in SL(2,\mathbb{Z})$ acting on the torus $\mathbb{R}^2/\mathbb{Z}^2$ by ordinary multiplication. The assumption that the entries are integers makes this well defined and the assumption that the determinant is one makes the action measure preserving with respect to the Lebesgue measure of the torus. If we assume that $|\operatorname{tr}(A)|>2$ (A is then called hyperbolic) the system will be chaotic. The quantization of a dynamical system is often divided into a quantization of the kinematics and a quantization of the dynamics, but for our purposes we are only interested in the quantization of the dynamics. This is a unitary operator $U_N(A)$ acting on the state space $L^2(\mathbb{Z}/N\mathbb{Z})$ with the inner product

$$\langle\phi,\psi\rangle=\frac{1}{N}\sum_{Q\in\mathbb{Z}_N}\phi(Q)\overline{\psi(Q)}.$$

The integer N plays the role of the inverse of Planck´s constant. In order for our quantization to be consistent with the quantization of the kinematics we will make the assumption that A is congruent to the identity modulo 2 and if N is even we assume that A is congruent to the identity modulo 4. Note that these assumptions does not tell us anything about the image of A in $SL(2,\mathbb{Z}_N)$ when N is odd, which will be the main concern in this paper. Let $N=p_1^{n_1}...p_m^{n_m}$. The Chinese remainder theorem gives us an isomorphism between $L^2(\mathbb{Z}_N)$ and $\bigotimes_{j=1}^m L^2\left(\mathbb{Z}_{p_j^{n_j}}\right)$. Using this decomposition we define $U_N(A):=\otimes_{j=1}^m U_{p_j^{n_j}}(A)$, where $U_{p_j^{n_j}}(A)$ is the Weil representation of the image of A in $SL(2,\mathbb{Z}_{p_j^{n_j}})$ for odd p and something similar for $p=2$. Let us first assume that p is odd and come back to the special case $p=2$ later. For odd p this representation of $SL(2,\mathbb{Z}_{p^n})$ is easiest to describe by its action on the elements

$$n_b=\begin{pmatrix}1&b\\0&1\end{pmatrix},\quad a_t=\begin{pmatrix}t&0\\0&t^{-1}\end{pmatrix}\text{ and }\ \omega=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$$

which generate the group. Before we write down the formulas for the action on the generators, let us first introduce some notation to simplify the expressions:

We will use the notation $e(x) = e^{i2\pi x}$ and denote the inverse of $2N/p^n$ modulo p^n by r. We will use the Legendre symbol $\left(\frac{t}{p}\right)$ and also write

$$\Lambda(t) = \left(\frac{t}{p}\right)^n$$

and

$$S_r\left(-1, p^n\right) = \begin{cases} 1 & \text{if } n \text{ is even} \\ \epsilon(p)\left(\frac{r}{p}\right) & \text{if } n \text{ is odd} \end{cases},$$

where

$$\epsilon(p) = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 4 \\ i \text{ if } p \equiv 3 \pmod 4 \end{cases}.$$

Definition 3.1. For odd p, U_{p^n} is the unique representation of $SL(2, \mathbb{Z}_{p^n})$ acting on $L^2(\mathbb{Z}_{p^n})$ satisfying

$$U_{p^n}(n_b)\psi(x) = e\left(\frac{rbx^2}{p^n}\right)\psi(x) \tag{1}$$

$$U_{p^n}(a_t)\psi(x) = \Lambda(t)\psi(tx) \tag{2}$$

$$U_{p^n}(\omega)\psi(x) = \frac{S_r\left(-1, p^n\right)}{\sqrt{p^n}} \sum_{y \in \mathbb{Z}_{p^n}} \psi(y) e\left(\frac{2rxy}{p^n}\right). \tag{3}$$

For $p = 2$ the construction is similar but one has to be very careful. First of all we identify A with its image in $SL(2, \mathbb{Z}_{2^{n+1}})$ and note that due to our assumption above we know that the image lies within the subgroup of matrices congruent to the identity modulo 4. This subgroup is generated by a_t, n_b, and n_c^T where $t \equiv 1 \pmod 4$ and $b \equiv c \equiv 0 \pmod 4$. We now define U_{2^n} acting on $L^2(\mathbb{Z}_{2^n})$ by

$$U_{2^n}(n_b)\psi(x) = e\left(\frac{rbx^2}{2^{n+1}}\right)\psi(x) \tag{4}$$

$$U_{2^n}(a_t)\psi(x) = \left(\frac{2}{t}\right)^n \psi(tx) \tag{5}$$

$$U_{2^n}(n_c^T) = H^{-1} U_{2^n}(n_{-c}) H, \tag{6}$$

where

$$H\psi(x) = \frac{1}{\sqrt{2^n}} \sum_{y \in \mathbb{Z}_{2^n}} \psi(y) e\left(\frac{rxy}{2^n}\right). \tag{7}$$

Hecke operators of quantized cat maps are often introduced in the language of algebraic number theory. Our definition is equivalent, but use a more well known vocabulary:

Definition 3.2. The Hecke operators corresponding to the matrix A are all the operators written as $U_N(g)$, where $g = xI + yA$ and g has determinant congruent to 1 modulo N. A function which is an eigenfunction of all Hecke operators is called a Hecke eigenfunction.

Definition 3.3. For $n \geqslant m \geqslant k$ we let

$$S_n(m,k) = \left\{ f \in L^2\left(\mathbb{Z}_{p^n}\right); p^m | x - y \Rightarrow f(x) = f(y) \ \wedge \ p^k \nmid x \Rightarrow f(x) = 0 \right\}.$$

In other words is $S_n(m,k)$ the set of all functions with period p^m and with support on the ideal $p^k\mathbb{Z}_{p^n}$. We are interested in these subspaces because of the following theorem in [16]:

Theorem 3.1. *Let p be an odd prime. $S_n(n-m,m)$ is invariant under the action of U_{p^n} and this action is isomorphic to the action of $U_{p^{n-2m}}$ on $L^2(\mathbb{Z}_{p^{n-2m}})$. The intertwining operator $T_m : S_n(n-m,m) \to L^2(\mathbb{Z}_{p^{n-2m}})$ is given by*

$$(T_m\psi)(x) = p^{-m/2}\psi(p^m x).$$

A Hecke eigenfunction $\psi \in L^2(\mathbb{Z}_{p^n})$ is called an oldform if $\psi \in S_n(n-1,1)$ and a newform if $\psi \in S_n(n-1,1)^{\perp}$. In the rest of this chapter and in Chapter 4 we will assume that $N = p^{2k+1}$, where p is an odd prime. Observe that many of our calculations will be done modulo p^k, and that this is something else than modulo N. We also make the assumption that A is not upper triangular modulo p.

In [16] we introduced a "preferred basis" in order to evaluate the newforms at specific points, this time we have to study more than just one basis. If we let δ_x denote the function $\delta_x : \mathbb{Z}_N \to \mathbb{C}$ which is 1 at x and 0 at every other point, the interesting functions can be defined by:

Definition 3.4. Given $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{Z}_N^2$ and $j \in \mathbb{F}_p$, let $\zeta_{j,x} : \mathbb{Z}_N \to \mathbb{C}$ be defined by

$$\zeta_{j,x} = \sum_{t\in\mathbb{Z}_{p^{k+1}}} e\left(\frac{rjt^2}{p}\right) e\left(\frac{x_1 t}{p^{k+1}}\right) \delta_{x_2+p^k t}.$$

Also define

$$\zeta_{\infty,x} = \sqrt{p} \sum_{t\in\mathbb{Z}_{p^k}} e\left(\frac{x_1 t}{p^k}\right) \delta_{x_2+p^{k+1}t}.$$

Remark. Note that the functions $\zeta_{j,x}$ are normalized so that $\|\zeta_{j,x}\|_2^2 = p^{-k}$.

In particular we can select two preferred orthogonal bases corresponding to $j = 0$ and $j = \infty$ in the definition. If $j = 0$ we let $x_1 \in \{1,2,...,p^{k+1}\}$ and $x_2 \in \{1,2,...,p^k\}$ and if $j = \infty$ we let $x_1 \in \{1,2,...,p^k\}$ and $x_2 \in \{1,2,...,p^{k+1}\}$. We will use the fact that if we pick other representatives for $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_{p^k}$ and $\mathbb{Z}_{p^k} \times \mathbb{Z}_{p^{k+1}}$ respectively, this only changes the functions by multiplication by a phase. Easy calculations, using disjointness of support and geometric sums, show the following lemma:

Lemma 3.2. *If $x \not\equiv x' \pmod{p^k}$ then $\langle \zeta_{j,x}, \zeta_{j',x'} \rangle = 0$.*

It was observed in [16] that the assumption made above stating that A is not upper triangular makes it possible for us to assume, without any further loss of generality, that the Hecke operators are given by $\{U_N(h); h \in H_D\}$, where H_D is defined by:

Definition 3.5. Given $D \in \mathbb{Z}_N$ we let

$$H_D = \left\{ \begin{pmatrix} a & bD \\ b & a \end{pmatrix} ; a,b \in \mathbb{Z}_N \ , \ a^2 - Db^2 = 1 \right\}.$$

We will use the following standard terminology from algebraic number theory: If D is a quadratic residue modulo p then A and all the matrices in H_D are diagonalizable modulo N and we say that p is split. If D is not a quadratic residue modulo p then it is not possible to diagonalize A or any matrix in H_D modulo N and we say that p is inert. Finally if $p|D$ then p is called ramified.

Definition 3.6. Let $\mathscr{N} : \mathbb{Z}_{p^k}^2 \to \mathbb{Z}_{p^k}$ be defined by $\mathscr{N}(x) = x_1^2 - Dx_2^2$.

Definition 3.7. For $C \in \mathbb{Z}_{p^k}$ we define

$$V_C = \bigoplus_{\substack{x \in \mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_{p^k} \\ \mathscr{N}(x) = -C}} \mathbb{C}\zeta_{0,x}.$$

Note that $S_{2k+1}(2k, 1) = \bigoplus_{p|x} \mathbb{C}\zeta_{0,x} \subseteq \bigoplus_{p^2|C} V_C$. On the other hand it is obvious that $\bigoplus_{p^2|C} V_C \subseteq \bigoplus_{p|C} V_C$, but if $x_1^2 - Dx_2^2 \equiv 0 \pmod{p}$ implies that $x \equiv 0 \pmod{p}$, i.e., if p is inert, then $\bigoplus_{p|C} V_C = \bigoplus_{p|x} \mathbb{C}\zeta_{0,x} = S_{2k+1}(2k, 1)$. Note also that Lemma 3.2 implies that $\zeta_{j,x} \in V_C$ iff $\mathscr{N}(x) = -C$.

Definition 3.8. For $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{F}_p)$ we let $T(B) : P^1(\mathbb{F}_p) \to P^1(\mathbb{F}_p)$ be defined by

$$j \mapsto \frac{aj + b}{cj + d}.$$

Remark. By this we mean that $\infty \mapsto a/c$ and that $T(B)j = \infty$ whenever the denominator is zero. Note that if the denominator is zero, then the numerator is nonzero.

4 Main calculations

We want to study the functions $\zeta_{j,x}$ because they transform in a simple manner when we act with $U_N(B)$.

Lemma 4.1. *Assume* $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}_N)$ *and let* $x' = Bx$. *Then* $U_N(B)\zeta_{j,x}$ *is equal to* $\zeta_{T(B)j,x'}$ *multiplied with some phase. If* $j \in \mathbb{F}_p$ *is such that* $p \nmid cj + d$ *we have that*

$$U_N(B)\zeta_{j,x} = \left(\frac{cj + d}{p}\right) e\left(\frac{r(x_1'x_2' - x_1x_2)}{N}\right) \zeta_{T(B)j,x'}.$$

Proof. The following identities are straightforward to check (similar calculations were done in [16]):

$$
\begin{aligned}
U_N(n_b)\zeta_{j,x} &= e\left(\frac{rbx_2^2}{N}\right)\zeta_{T(n_b)j,n_bx} && \forall j \in P(\mathbb{F}_p)\\
U_N(a_t)\zeta_{j,x} &= \left(\frac{t}{p}\right)\zeta_{T(a_t)j,a_tx} && \forall j \in P(\mathbb{F}_p)\\
U_N(\omega)\zeta_{j,x} &= \left(\frac{j}{p}\right)e\left(\frac{-x_1x_2}{N}\right)\zeta_{T(\omega)j,\omega x} && \forall j \in \mathbb{F}_p^\times\\
U_N(\omega)\zeta_{0,x} &= \left(\frac{2}{p}\right)\epsilon(p)e\left(\frac{-x_1x_2}{N}\right)\zeta_{\infty,\omega x}\\
U_N(\omega)\zeta_{\infty,x} &= \left(\frac{2}{p}\right)\epsilon(p)e\left(\frac{-x_1x_2}{N}\right)\zeta_{0,\omega x}
\end{aligned}
$$

Since all elements in $SL(2,\mathbb{Z}_N)$ can be written as a product of n_b, a_t and ω, the first part of the lemma follows directly. To prove the second part we note that the identity holds for the generators and that both sides of the equality is multiplicative. However the identity holds only for $j \neq \infty$ and $p \nmid cj+d$. This means that if we think of $U_N(B)$ as a product of $U_N(n_b), U_N(a_t)$ and $U_N(\omega)$, and try to apply the identity above we might run into trouble if the "new" j does not have this property. Looking through the table above, it is easy to see that the only time that this can happen is if we are forced to apply $U_N(\omega)$ to $\zeta_{0,x}$. But since the result at the end will be some phase times $\zeta_{j',x'}$, where $j' \neq \infty$, we know that we later must apply $U_N(\omega)$ to some $\zeta_{\infty,x''}$ (once again looking through the table above). From this it is easy to realize that it is enough to check that $U_N(\omega)U_N(B')U_N(\omega)\zeta_{0,x}$ is what it should be for all B' which is a product of matrices of the form n_b and a_t (i.e. upper triangular with determinant one). But such matrices can be written as just n_ba_t, thus it is enough to show that

$$U_N(\omega)U_N(n_b)U_N(a_t)U_N(\omega)\zeta_{0,x} = \left(\frac{-t}{p}\right)e\left(\frac{r(x_1'x_2'-x_1x_2)}{N}\right)\zeta_{0,\omega n_ba_t\omega x}.$$

Observing that

$$\epsilon(p)^2 = \left(\frac{-1}{p}\right)$$

and applying the identities above this is straightforward. □

We see that these functions behave a lot like the ζ_x−functions in [16] (see Lemma 5.1 in [16] for details). The difference is that we now have to introduce the extra parameter j. The main problem is how to use the theory for ζ_x−functions even though we have this new parameter. The ζ_x−functions were similar to the functions studied by Knabe [11] and he offers a solution to this problem in a special case: He only studied the case when N is a square, but in the end of the paper, he remarks that his construction can be carried out, not only if N is a square, but also if A has an eigenvector modulo N. In our language this corresponds to the case that p is not inert and this can be seen also in our case because if p is not inert there exists some $j_0 \in P^1(\mathbb{F}_p)$ such that $T(h)j_0 = j_0$ for all $h \in H_D$. That means that the basis $\zeta_{j_0,x}$ is transformed to itself as the ζ_x−basis did. The case $j_0 = 0$ is equivalent to p ramified, $j_0 = \infty$ is equivalent to A upper triangular modulo p and if $j_0 \in \mathbb{F}_p^\times$ p is split. Note that if p is inert no such j_0 exist. The main disadvantage with this approach is that there seem to be no way to handle the inert case with this method. Since we want a general theorem we will instead use Lemma 4.3 to handle the problems caused by j.

We also note the resemblance between our functions and the basis studied by Degli Esposti et al in [5, 6]. They also study the situation where A has an eigenvector modulo N.

Corollary 4.2. *If $\psi \in V_C$, then*

$$U_N \begin{pmatrix} 1 & tp^{k+1}D \\ tp^{k+1} & 1 \end{pmatrix} \psi = e\left(\frac{rCt}{p^k}\right)\psi.$$

Proof. ψ can be written as a linear combination of $\zeta_{0,x}$ such that $\mathscr{N}(x) = -C$. Put $x' = \begin{pmatrix} 1 & tp^{k+1}D \\ tp^{k+1} & 1 \end{pmatrix} x$. We see that

$$\begin{aligned} U_N \begin{pmatrix} 1 & tp^{k+1}D \\ tp^{k+1} & 1 \end{pmatrix} \zeta_{0,x} &= e\left(\frac{r(x_1'x_2' - x_1x_2)}{N}\right)\zeta_{0,x'} \\ &= e\left(\frac{r\left(x_1^2 + Dx_2^2\right)t}{p^k}\right) \sum_{s\in\mathbb{Z}_{p^{k+1}}} e\left(\frac{\left(x_1 + tp^{k+1}Dx_2\right)s}{p^{k+1}}\right)\delta_{x_2+tp^{k+1}x_1+sp^k} \\ &= e\left(\frac{r\left(x_1^2 + Dx_2^2\right)t}{p^k}\right) \sum_{s\in\mathbb{Z}_{p^{k+1}}} e\left(\frac{x_1\left(s - tpx_1\right)}{p^{k+1}}\right)\delta_{x_2+sp^k} \\ &= e\left(-\frac{r\mathscr{N}(x)t}{p^k}\right)\zeta_{0,x}, \end{aligned}$$

from which the statement follows. □

In the rest of this chapter we will assume that $N = p^{2k+1}$ fulfills that $k > 0$, i.e., that N is not a prime.

Lemma 4.3. *If ψ is a normalized Hecke eigenfunction then there exists an element $C \in \mathbb{Z}_{p^k}$ such that $\psi \in V_C$. If p neither divides C nor D, then the following holds:*

1. *For all $\zeta_{0,x} \in V_C$ such that $p \nmid x_2$ we have*

$$|\langle\psi, \zeta_{0,x}\rangle| = \frac{1}{\sqrt{p^{2k+1} - \left(\frac{D}{p}\right)p^{2k}}}.$$

2. *For all $\zeta_{\infty,x} \in V_C$ such that $p \nmid x_1$ we have*

$$|\langle\psi, \zeta_{\infty,x}\rangle| = \frac{1}{\sqrt{p^{2k+1} - \left(\frac{D}{p}\right)p^{2k}}}.$$

Proof. That $\psi \in V_C$ for some C follows directly from Corollary 4.2 since an eigenfunction can not be a sum of eigenfunctions corresponding to different eigenvalues. For $y \in \mathbb{Z}_p^2$, let ψ_y denote the projection of ψ onto the space

$$\bigoplus_{x \equiv y \pmod p} \mathbb{C}\zeta_{0,x}.$$

We observe that ψ_y is the zero function unless $\mathscr{N}(y) \equiv -C \pmod p$, in other words $\psi = \sum \psi_y$, where the sum is taken over the elements in $\mathbb{Z}_p^2$ such that $\mathscr{N}(y) \equiv -C \pmod p$. These y form an orbit since if y and y' fulfill $\mathscr{N}(y) \equiv \mathscr{N}(y') \equiv -C \pmod p$ then there exists an $h \in H_D$ such that h is congruent to $\begin{pmatrix} x_1' & x_2'D \\ x_2' & x_1' \end{pmatrix} \begin{pmatrix} x_1 & x_2D \\ x_2 & x_1 \end{pmatrix}^{-1}$ modulo p. This matrix maps y to y' and this shows that the elements actually form an orbit of H_D, i.e., they can be written as $H_D y$ for some y. We now show that all ψ_y have the same L^2-norm for y such that $\mathscr{N}(y) \equiv -C \pmod p$. Write ψ_y as a linear combination of $\zeta_{0,x}$, where $x \equiv y \pmod p$, and apply $U_N(h)$. Lemma 4.1 tells us that this is a linear combination of $\zeta_{T(h)0,hx}$ and by Lemma 3.2 we know that $\langle \psi_{y'}, \zeta_{T(h)0,hx}\rangle = 0$ unless $y' \equiv hx \pmod p$. From this we see that $\langle \psi_{y'}, U_N(h)\psi_y\rangle = 0$ unless $y' \equiv hx \pmod p$. On the other hand ψ is a Hecke eigenfunction, and from this we may now deduce that the image of $U_N(h)\psi_y$ is ψ_{hy} times some phase and moreover, since the elements form an orbit, that $\|\psi_y\|_2$ is independent of y. One argument for this is the following: We see that

$$\begin{aligned} \|\psi\|_2^2 &= |\langle \psi, U_N(h)\psi\rangle| = \left|\left\langle \sum \psi_y, \sum U_N(h)\psi_y \right\rangle\right| = \left|\sum \langle \psi_{hy}, U_N(h)\psi_y\rangle\right| \\ &\leqslant \sum |\langle \psi_{hy}, U_N(h)\psi_y\rangle| \leqslant \sum \|\psi_{hy}\|_2 \|U_N(h)\psi_y\|_2 = \sum \|\psi_{hy}\|_2\|\psi_y\|_2 \\ &\leqslant \sqrt{\sum \|\psi_{hy}\|_2^2}\sqrt{\sum \|\psi_y\|_2^2} = \|\psi\|_2\|\psi\|_2, \end{aligned}$$

applying the triangle inequality once and the Cauchy-Schwarz inequality twice. Obviously all inequalities are actually equalities and equality in the last inequality is obtained if and only if $\|\psi_{hy}\|_2 = \|\psi_y\|_2$ for all y. We now know that $\|\psi_y\|_2 = A$, where A^{-2} is the number of solutions to $y_1^2 - Dy_2^2 \equiv -C \pmod p$. In the proof of Lemma 5.3 in [16] this number was calculated to be $p - \left(\frac{D}{p}\right)$, thus $\|\psi_y\|_2 = \left(p - \left(\frac{D}{p}\right)\right)^{-1/2}$. Let us now turn our attention to $\psi_y = \sum a_x \zeta_{0,x}$ and assume that $p \nmid y_2$, the sum is over elements in $\mathbb{Z}_N^2$ representing the different elements in $\mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_{p^k}$ such that $x \equiv y \pmod p$ and $\mathscr{N}(x) = -C$. Once again referring to the proof of Lemma 5.3 in [16] it is easy to understand that the number of terms in this sum is independent of y. Moreover, summing over all y, we must have $p^k \left(p - \left(\frac{D}{p}\right)\right)$ terms in total. Thus the sum $\psi_y = \sum a_x \zeta_{0,x}$ must have p^k terms, since the number of y was $p - \left(\frac{D}{p}\right)$. If we can prove that all coefficients a_x have the same absolute value, it is an easy calculation to show claim 1. To do this we show that given x, x' such that $\mathscr{N}(x) = \mathscr{N}(x') = -C$ and $x \equiv x' \equiv y \pmod p$ there is an element $h \in H_D$ such that $U_N(h)\zeta_{0,x}$ is equal to $\zeta_{0,x'}$ up to a phase. We know that $x_1^2 - Dx_2^2 \equiv x_1'^2 - Dx_2'^2 \pmod{p^k}$, but in general these expressions are not equal modulo p^{k+1}. However the $\zeta_{0,x}-$function is equal up to multiplication by a phase when we change x_2 by adding tp^k.

Since $x_2' \not\equiv 0 \pmod{p}$ we see that we can change x_2' in this manner so that $x_1^2 - Dx_2^2 \equiv x_1'^2 - Dx_2'^2 \pmod{p^{k+1}}$. We can now define $h \in H_D$ so that

$$h \equiv \begin{pmatrix} x_1' & x_2'D \\ x_2' & x_1' \end{pmatrix} \begin{pmatrix} x_1 & x_2 D \\ x_2 & x_1 \end{pmatrix}^{-1} \pmod{p^{k+1}}.$$

We see that $hx \equiv x' \pmod{p^{k+1}}$, but moreover $h \equiv \mathrm{Id} \pmod{p}$, which gives $T(h)0 = 0$. Using Lemma 4.1 we can conclude that in fact $U_N(h)\zeta_{0,x}$ is equal to $\zeta_{0,x'}$ up to a phase. Claim 2 is proven is the same manner but ψ_y is written in a $\zeta_{\infty,x}-$basis and x_1' is changed instead of x_2'. □

The following three theorems will give us exact expressions for the value of the Hecke eigenfunctions at all different points $b \in \mathbb{Z}_N$ such that the equation $x^2 \equiv -C + Db^2 \pmod{p^k}$ has solutions. The expressions are sums over these solutions and the value of a Hecke eigenfunction at a point $b \in \mathbb{Z}_N$ such that $-C + Db^2$ is a quadratic non-residue is zero (because the sum is empty). Note that all Hecke eigenfunctions seem to behave very similar to each other in the sense that they take more or less the same values, but at different points. If two Hecke eigenfunctions lie in the same space V_C, they are even more similar, the expressions in the theorems applies to all these newforms simultaneously. Let us also note that the expressions are rather surprising, if we compare them to most of the previous results, in the sense that they do not distinguish the cases p split and p inert, except for the normalization constant. On the other hand they are perhaps not so surprising in the sense that they are very similar to the corresponding theorems for even prime powers proven in [16]. The first theorem handles most of the points $b \in \mathbb{Z}_N$ where $-C + Db^2$ is a square, i.e. where $\psi(b) \neq 0$. In fact, if CD^{-1} is a quadratic non-residue, then it handles all b in the support of ψ.

Theorem 4.4. *Let $\psi \in V_C$ be a normalized Hecke eigenfunction and assume that p does not divide C or D. Let b fulfill that $-C + Db^2 \equiv x_0^2 \pmod{p^k}$ for some $p \nmid x_0$. Then*

$$\psi(b) = \frac{1}{\sqrt{1 - \left(\frac{D}{p}\right)\frac{1}{p}}}(\alpha_\psi(b) + \beta_\psi(b)),$$

where α_ψ and β_ψ are functions satisfying $|\alpha_\psi(b)| = |\beta_\psi(b)| = 1$, $\alpha_\psi(b+p^{k+1}t) = e\left(\frac{x_0 t}{p^k}\right)\alpha_\psi(b)$ and $\beta_\psi(b + p^{k+1}t) = e\left(\frac{-x_0 t}{p^k}\right)\beta_\psi(b)$.

Proof. This follows directly from the fact that ψ can be written as

$$\psi = \sum_{\mathscr{N}(x) = -C} a_x \zeta_{\infty,x}$$

with $|a_x| = \left(p - \left(\frac{D}{p}\right)\right)^{-1/2}$ for those x such that $p \nmid x_1$. □

The next theorem is a generalization of the previous in the sense that Theorem 4.4 corresponds to $s = 0$. To see that the two expressions agree you have to observe that Theorem 4.5 reduces to a sum of two Gauss sums if $s = 0$ (because the coefficient is zero in front of z^3) and evaluate these. To get this exact form we must assume $p > 3$ when $s > (k-1)/3$. A similar theorem may easily be obtained also for $p = 3$, the only difference between the proofs are the expressions for $B(s)^z$.

Theorem 4.5. *Let $\psi \in V_C$ be a normalized Hecke eigenfunction and assume that p does not divide C or D. Let $b \in \mathbb{Z}_N^\times$ and assume that the equation $y^2 \equiv -C + Db^2 \pmod{p^k}$ has the solutions $y \equiv \pm x_0 p^s + p^{k-s}\mathbb{Z}_{p^s} \pmod{p^k}$ for some x_0 and s such that $p \nmid x_0$ and $0 \leqslant s < k/2$. Then*

$$\psi(b) = \frac{1}{\sqrt{p - \left(\frac{D}{p}\right)}} \left(\alpha_\psi(b) \sum_{z=1}^{p^{s+1}} e\left(\frac{q_+(z)}{p^{s+1}}\right) + \beta_\psi(b) \sum_{z=1}^{p^{s+1}} e\left(\frac{q_-(z)}{p^{s+1}}\right) \right), \tag{8}$$

where $q_\pm(z) = r\left(\Theta_\psi(b)z \pm x_0 Dbz^2 + p^{k-2s}3^{-1}D^2b^2z^3\right)$ and $|\alpha_\psi(b)| = |\beta_\psi(b)| = 1$. The function $\Theta_\psi(b)$ is given by

$$\Theta_\psi(b)p^k \equiv -x_0^2p^{2s} - \widetilde{C} + Db^2 - p^{2(k-s)}3^{-1}rD^2b^2 \pmod{p^{k+s+1}}. \tag{9}$$

Remark. Since $\widetilde{C}$ is some integer (dependent on ψ) congruent to C modulo p^k it is easy to see that $\Theta_\psi(b)$ is well defined, but that it can not be lifted to an integer polynomial. Further more, the proof will show that different Hecke eigenfunctions in V_C correspond to different choices of $\widetilde{C} \equiv C \pmod{p^k}$.

Proof. We know that ψ is a linear combination of $\zeta_{0,x}$ such that $\mathscr{N}(x) = -C$ and that the coefficients where $p \nmid x_2$ all have absolute value

$$p^k|\langle \psi, \zeta_{0,x}\rangle| = \frac{1}{\sqrt{p - \left(\frac{D}{p}\right)}}.$$

Since $\zeta_{0,x}(b) = 0$ unless $x_2 \equiv b \pmod{p^k}$ the value of $\psi(b)$ is only a sum over $x \in \mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_{p^k}$ such that $x_1^2 \equiv -C + Db^2 \pmod{p^k}$ and $x_2 \equiv b \pmod{p^k}$. By the assumptions of the theorem we have that $x_1 \equiv \pm x_0 p^s + p^{k-s}\mathbb{Z}_{p^{s+1}} \pmod{p^{k+1}}$. Let $B(s) = \begin{pmatrix} 1 + rDp^{2(k-s)} & p^{k-s}D \\ p^{k-s} & 1 + rDp^{2(k-s)} \end{pmatrix}$. The main observation is that the x we want to sum over are generated as two different orbits of $B(s)$ in the sense that the x can be represented by the elements

$$\left\{ B(s)^z \begin{pmatrix} x_0p^s \\ b \end{pmatrix}; z = 0, 1, ..., p^{s+1}-1 \right\} \cup \left\{ B(s)^z \begin{pmatrix} -x_0p^s \\ b \end{pmatrix}; z = 0, 1, ..., p^{s+1}-1 \right\}$$

in $\mathbb{Z}_N^2$. By induction it is easy to show that

$$B(s)^z = \begin{pmatrix} 1 + rDz^2p^{2(k-s)} & \left(p^{k-s}z + 3^{-1}rDp^{3(k-s)}(z^3 - z)\right)D \\ p^{k-s}z + 3^{-1}rDp^{3(k-s)}(z^3 - z) & 1 + rDz^2p^{2(k-s)} \end{pmatrix}.$$

Denote $\zeta_{\pm,z} = \zeta_{0,B(s)^z\binom{\pm x_0p^s}{b}}$ and call the constants in front of these functions $a_{\pm,z}\left(p - \left(\frac{D}{p}\right)\right)^{-1/2}$. We have that

$$\psi(b) = \frac{1}{\sqrt{p - \left(\frac{D}{p}\right)}} \left(\sum_{z=0}^{p^{s+1}-1} a_{+,z}\zeta_{+,z}(b) + \sum_{z=0}^{p^{s+1}-1} a_{-,z}\zeta_{-,z}(b) \right).$$

If we use Lemma 4.1 we see that $U_N(B(s))\zeta_{\pm,z-1} = e\left(\frac{r(f_\pm(z)-f_\pm(z-1))}{N}\right)\zeta_{\pm,z}$ for $z = 1, ..., p^{s+1} - 1$, where

$$\begin{aligned} f_\pm(z) &= \left(\pm\left(1 + rDz^2p^{2(k-s)}\right)p^s x_0 + \left(p^{k-s}z + 3^{-1}rDp^{3(k-s)}(z^3 - z)\right)Db\right) \\ &\quad\times\left(\pm\left(p^{k-s}z + 3^{-1}rDp^{3(k-s)}(z^3 - z)\right)p^s x_0 + \left(1 + rDz^2p^{2(k-s)}\right)b\right) \\ &\equiv \pm p^s x_0 b + p^{k-s}\left(Db^2 + p^{2s}x_0^2 - p^{2(k-s)}3^{-1}rD^2b^2\right)z \\ &\quad\pm p^{2k-s}2x_0Dbz^2 + p^{3(k-s)}3^{-1}2D^2b^2z^3 \qquad\qquad (\text{mod } N). \end{aligned}$$

Since $B(s)^{p^{s+1}} = \begin{pmatrix} 1 & p^{k+1}D \\ p^{k+1} & 1 \end{pmatrix}$ Corollary 4.2 gives us that $U_N(B(s))\psi = e\left(\frac{r\widetilde{C}}{p^{k+s+1}}\right)\psi$ for some $\widetilde{C} \equiv C \pmod{p^k}$ and this leads to

$$\begin{aligned} a_{\pm,z} &= e\left(\frac{-r\widetilde{C}}{p^{k+s+1}}\right)e\left(\frac{r\left(f_\pm(z) - f_\pm(z-1)\right)}{N}\right)a_{\pm,z-1} \\ &= e\left(\frac{-r\widetilde{C}z}{p^{k+s+1}}\right)e\left(\frac{r\left(f_\pm(z) - f_\pm(0)\right)}{N}\right)a_{\pm,0}. \end{aligned}$$

But $\zeta_{\pm,z}(b) = e\left(\frac{-p^{k+s}x_0^2z\mp p^{2k-s}3rx_0Dbz^2-p^{3(k-s)}rD^2b^2z^3}{N}\right)$ hence

$$\begin{aligned} a_{\pm,z}\zeta_{+,z}(b) &= e\left(\frac{-p^{k-s}r\widetilde{C}z + rf_\pm(z) - rf_\pm(0) - p^{k+s}x_0^2z}{N}\right) \\ &\quad\times e\left(\frac{\mp p^{2k-s}3rx_0Dbz^2 - p^{3(k-s)}rD^2b^2z^3}{N}\right)a_{\pm,0} = a_{\pm,0}e\left(\frac{q_\pm(z)}{p^{s+1}}\right), \end{aligned}$$

where $q_\pm(z) = r\left(\Theta_\psi(b)z \pm x_0Dbz^2 + p^{k-2s}3^{-1}D^2b^2z^3\right)$ and

$$\Theta_\psi(b)p^k \equiv -x_0^2p^{2s} - \widetilde{C} + Db^2 - p^{2(k-s)}3^{-1}rD^2b^2 \pmod{p^{k+s+1}}.$$

□

The last of the evaluation theorems concerns the case when the number of solutions to $x^2 \equiv -C + Db^2$ (mod p^k) is maximal, i.e. when $-C + Db^2 \equiv 0$ (mod p^k). For this to happen we must have that CD^{-1} is a non-zero square modulo p. Maximal number of solutions leads to the maximal number of terms in the sum and as we shall see in Chapter 5, this is also the case that gives the supremum norm.

Theorem 4.6. *Let $N = p^{2k+1}$, where $p > 3$ and $k > 0$. Let $\psi \in V_C$ be a normalized Hecke eigenfunction for some $C \in \mathbb{Z}_{p^k}^\times$. If $b \in \mathbb{Z}_N$ fulfills that $-C + Db^2 \equiv 0 \pmod{p^k}$ then*

$$\psi(b) = \frac{\alpha_\psi(b)}{\sqrt{p - \left(\frac{D}{p}\right)}}\sum_{z=1}^{p^{[k/2]+1}} e\left(\frac{q(z)}{p^{[k/2]+1}}\right), \tag{10}$$

where $q(z) = \Theta_\psi(b)z - p^{k-2[k/2]}3^{-1}2CDz^3$, $|\alpha_\psi(b)| = 1$ *and*

$$\Theta_\psi(b)p^k \equiv -\widetilde{C} + Db^2 - p^{2\lceil k/2\rceil}3^{-1}CD \pmod{p^{[3k/2]+1}}.$$

Proof. To prove this result we have to adjust the proof of Theorem 4.5 slightly, but the ideas are the same. Denote $\alpha = p^{\lceil k/2\rceil}$. We know that $\alpha^5 \equiv 0 \pmod{N}$. We put

$$B = \begin{pmatrix} 1+2D\alpha^2 & (2\alpha + D\alpha^3)D \\ 2\alpha + D\alpha^3 & 1+2D\alpha^2 \end{pmatrix}$$

and notice that ψ can be written as a linear combination of $\zeta_{0,x}$ where $x = B^z \begin{pmatrix} 0 \\ b \end{pmatrix}$ and $z = 0, 1, 2, ..., p^{[k/2]+1} - 1$. If we calculate this explicitly we get

$$B^z = \begin{pmatrix} 1 + 2Dz^2\alpha^2 + 3^{-1}2D^2z^2(z^2-1)\alpha^4 & (2z\alpha + 3^{-1}Dz(4z^2-1)\alpha^3)D \\ 2z\alpha + 3^{-1}Dz(4z^2-1)\alpha^3 & 1 + 2Dz^2\alpha^2 + 3^{-1}2D^2z^2(z^2-1)\alpha^4 \end{pmatrix}$$

and

$$B^z \begin{pmatrix} 0 \\ b \end{pmatrix} = \begin{pmatrix} 2Dbz\alpha + 3^{-1}D^2bz(4z^2-1)\alpha^3 \\ b + 2Dbz^2\alpha^2 + 3^{-1}2D^2bz^2(z^2-1)\alpha^4 \end{pmatrix}.$$

Denote $\xi_z = \zeta_{0,B^z\binom{0}{b}}$. We can write $\psi(b)$ as

$$\psi(b) = \frac{1}{\sqrt{p - \left(\frac{D}{p}\right)}} \sum_{z=0}^{p^{[k/2]+1}-1} a_z \xi_z(b)$$

and since $B^{p^{[k/2]+1}} = \begin{pmatrix} 1 & 2p^{k+1}D \\ 2p^{k+1} & 1 \end{pmatrix}$, Corollary 4.2 tells us that $U_N(B)\psi = e\left(\frac{\widetilde{C}}{p^{[3k/2]+1}}\right)\psi$ for some $\widetilde{C} \equiv C \pmod{p^k}$. This leads to the the relation

$$a_z = e\left(\frac{((-\widetilde{C} + Db^2)\alpha - 3^{-1}D^2b^2\alpha^3)z + 3^{-1}10D^2b^2\alpha^3z^3}{p^{2k+1}}\right)$$

in the same manner as before. Evaluating $\xi_z(b)$ gives:

$$\xi_z(b) = e\left(\frac{-4D^2b^2\alpha^3z^3}{p^{2k+1}}\right)$$

By the definition of Θ_ψ we have

$$\Theta_\psi(b)p^k \equiv -\widetilde{C} + Db^2 - 3^{-1}CDp^{2\lceil k/2\rceil} \pmod{p^{[3k/2]+1}}$$

and $C \equiv Db^2 \pmod{p^k}$ and this gives the desired formula. □

5 Results and the proof of Theorem 1.1

In this chapter we will prove the same theorems as we did in [16], but this time when $N = p^n$ and n is odd instead of even. Note that V_C is defined in slightly different manners when n is even or odd, but that it is philosophically the same object.

Let us first recall some definitions and properties of exponential sums of cubic polynomials from Chapter 6 in [16] which we will need in the proof of Theorem 5.3:

Definition 5.1. Let n be a nonnegative integer. For $q \in \mathbb{Z}_{p^n}[x]$ we define

$$S(q,n) = \sum_{z=1}^{p^n} e\left(\frac{q(z)}{p^n}\right).$$

Definition 5.2. For $\alpha \in \mathbb{Z}_{p^n}^\times$ and $n = 1$ or $n = 2$ we define

$$A_{\alpha,n} = \frac{\sup_{t \in \mathbb{Z}_{p^n}} |S(q_{\alpha,t}, n)|}{p^{n/2}},$$

where $q_{\alpha,t}(z) = \alpha z^3 + tz$.

Remark. $A_{\alpha,n}$ is bounded by 2 and for fixed n and p, $A_{\alpha,n}$ assumes at most three different values. If $p \equiv 2 \pmod 3$ then $A_{\alpha,n}$ is independent of α.

We will use the following theorem:

Theorem 5.1. *Let $p > 3$. If $q_{\alpha,t}(z) = \alpha z^3 + tz$ and $\alpha \in \mathbb{Z}_{p^n}^\times$ then*

$$\sup_{t \in \mathbb{Z}_{p^n}} |S(q_{\alpha,t}, n)| = \begin{cases} p^{2n/3} & \text{if } n \equiv 0 \pmod 3 \\ A_{\alpha,1} p^{2n/3-1/6} & \text{if } n \equiv 1 \pmod 3 \\ A_{\alpha,2} p^{2n/3-1/3} & \text{if } n \equiv 2 \pmod 3 \end{cases}.$$

Let us also recapitulate the meaning of the two parameters C and D. D is directly determined by A, but C parameterizes the Hecke eigenfunctions and different C corresponds to different characters on the dual of the Hecke group. The "generic" values of C and D (the values such that $p \nmid C, D$) corresponds to the cases when the eigenspaces of the characters are one dimensional and to the case when A has zero or two linearly independent eigenvectors modulo p. Our main concern is these "generic" values and the two theorems given below calculates the supremum norm of the "generic" newforms of a "generic" Hecke group. If p is inert all newforms are "generic", but if p is split there are newforms such that $p|C$. In both pictures of Figure 2 in the introduction we see two lines, one corresponding to the newforms covered by Theorem 5.2 and one corresponding to the newforms covered by Theorem 5.3. The main difference between the two pictures in Figure 2 is the "noise" in the left picture coming from the "non-generic" newforms. Since there are no "non-generic" newforms in the inert case there is no noise in the right picture.

Theorem 5.2. *Let $N = p^n$ for some odd prime p that does not divide C or D and assume that $\psi \in V_C$ is a normalized Hecke eigenfunction. If $\left(\frac{C}{p}\right) = -\left(\frac{D}{p}\right)$ then*

$$\frac{2}{\sqrt{1 - \left(\frac{D}{p}\right)\frac{1}{p}}}\left(1 - \frac{\pi^2}{8p^{2[n/2]}}\right) \leqslant \|\psi\|_\infty \leqslant \frac{2}{\sqrt{1 - \left(\frac{D}{p}\right)\frac{1}{p}}}.$$

Remark. We allow $n = 1$ in the theorem although $p \nmid C$ does not make any sense in this situation (C is defined modulo 1).

Proof. For $n = 1$ the estimates from above are well known [14, 12] and the estimates from below are trivial. For even n this theorem was proven in [16] (the case $p = 3$ is not included in the corresponding theorem, but the proof does not use that $p \neq 3$ in any significant way), thus it remains to prove it for odd $n \geqslant 3$. Let us therefore write $n = 2k + 1$, for some positive integer k. We see that if $\left(\frac{C}{p}\right) = -\left(\frac{D}{p}\right)$ then $-C + Db^2 \not\equiv 0 \pmod{p}$ for all b, hence Theorem 4.4 immediately gives

$$\|\psi\|_\infty \leqslant \frac{2}{\sqrt{1 - \left(\frac{D}{p}\right)\frac{1}{p}}}. \tag{11}$$

The other inequality also follows easily from Theorem 4.4 by picking a $b \in \mathbb{Z}_N$ such that $\left(\frac{-C+Db^2}{p}\right) = 1$ and changing b by adding tp^{k+1} to maximize the expression in the same manner as was done in the proof of the corresponding theorem (Theorem 7.1) in [16]. The idea used is that the absolute value of the sum of two phases is as large as possible, when the difference between the arguments of the phase is as small as possible. To find the maximal minimal difference one uses the pigeon hole principle. □

Theorem 5.3. *Let $N = p^n$ for some prime $p > 3$ and some $n \geqslant 3$. If $\psi \in V_C$ is a normalized Hecke eigenfunction for some $C \in \mathbb{Z}_{p^n}^\times$ and $\left(\frac{C}{p}\right) = \left(\frac{D}{p}\right)$ then*

$$\|\psi\|_\infty = \frac{N^{1/6}}{\sqrt{1 - \left(\frac{D}{p}\right)\frac{1}{p}}} \times \begin{cases} 1 & \textit{if } n \equiv 0 \pmod{3} \\ A_{\alpha,1}p^{-1/6} & \textit{if } n \equiv 1 \pmod{3} \\ A_{\alpha,2}p^{-1/3} & \textit{if } n \equiv 2 \pmod{3} \end{cases}, \tag{12}$$

where $\alpha = 36CD$ when n is even and $\alpha = 18CD$ when n is odd.

Proof. This theorem was proven for even n in [16], the proof for odd n is very similar. Let $n = 2k + 1$. We want to show that the maximal value of the expression in Theorem 4.6 is the value in (12) and that the expressions in Theorem 4.4 and Theorem 4.5 are smaller. The absolute value of the expression in Theorem 4.4 is obviously less or equal than $2\left(1 - \left(\frac{D}{p}\right)\frac{1}{p}\right)^{-1/2}$ and this is smaller than (12). Using Lemma 6.2 in [16] the expression in Theorem 4.5 (Equation (8)) can be estimated by

$$\frac{2p^{(s+1)/2}}{\sqrt{p - \left(\frac{D}{p}\right)}} = \frac{2p^{s/2}}{\sqrt{1 - \left(\frac{D}{p}\right)\frac{1}{p}}}$$

and $s \leqslant (n-3)/4$. Recalling that $A_{3^{-1}rCD,2} > \sqrt{2}$ and $A_{3^{-1}rCD,1} > 1$ it is easy to see that this is less than the expression in (12). The absolute value of the expression in Theorem 4.6 is

$$|\psi(b)| = \left(p - \left(\frac{D}{p}\right)\right)^{-1/2} |S(q, [k/2] + 1)|,$$

where $q(z) = \Theta_\psi(b)z - p^{k-2[k/2]}3^{-1}2CDz^3$. If we change b by adding tp^k the only thing that changes in (10) is $\Theta_\psi(b)$ and this change is easily calculated to be $\Theta_\psi(b + tp^k) \equiv \Theta_\psi(b) + 2Dbt \pmod{p^{[k/2]+1}}$. Since $p \nmid 2Db$ we see that the largest possible value of $\psi(b + tp^k)$ is

$$\frac{1}{\sqrt{p - \left(\frac{D}{p}\right)}} \sup_{t \in \mathbb{Z}_{[k/2]+1}} |S(q_{\alpha,t}, [k/2] + 1)|,$$

where $q_{\alpha,t}(z) = \alpha z^3 + tz$ and $\alpha = -p^{k-2[k/2]}3^{-1}2CD$. If k is even we may apply Theorem 5.1 to get that

$$\begin{aligned} \|\psi\|_\infty &= \frac{1}{\sqrt{p - \left(\frac{D}{p}\right)}} \begin{cases} p^{2/3(k/2+1)} & \text{if } k/2 + 1 \equiv 0 \pmod 3 \\ A_{\alpha,1}p^{2/3(k/2+1)-1/6} & \text{if } k/2 + 1 \equiv 1 \pmod 3 \\ A_{\alpha,2}p^{2/3(k/2+1)-1/3} & \text{if } k/2 + 1 \equiv 2 \pmod 3 \end{cases} \\ &= \frac{1}{\sqrt{1 - \left(\frac{D}{p}\right)\frac{1}{p}}} \begin{cases} p^{n/6} & \text{if } n \equiv 0 \pmod 3 \\ A_{\alpha,1}p^{n/6-1/6} & \text{if } n \equiv 1 \pmod 3 \\ A_{\alpha,2}p^{n/6-1/3} & \text{if } n \equiv 2 \pmod 3 \end{cases} \end{aligned}$$

and $A_{-3^{-1}2CD,n} = A_{18CD,n}$. If k is odd we see that $p|\alpha$ and if $p \nmid t$ then $q'_{\alpha,t}(z) \equiv t \not\equiv 0 \pmod p$. Linearizing in the same manner as was done repeatedly in chapter 6 of [16], it is easy to see that $S(q_{\alpha,t}, [k/2] + 1) = 0$. Thus writing $t = p\tilde{t}$ and $\alpha = p\tilde{\alpha}$ we get

$$\begin{aligned} \|\psi\|_\infty &= \frac{p}{\sqrt{p - \left(\frac{D}{p}\right)}} \sup_{\tilde{t} \in \mathbb{Z}_{[k/2]}} |S(q_{\tilde{\alpha},\tilde{t}}, [k/2])| \\ &= \frac{1}{\sqrt{p - \left(\frac{D}{p}\right)}} \begin{cases} p^{1+(k-1)/3} & \text{if } (k-1)/2 \equiv 0 \pmod 3 \\ A_{\tilde{\alpha},1}p^{1+(k-1)/3-1/6} & \text{if } (k-1)/2 \equiv 1 \pmod 3 \\ A_{\tilde{\alpha},2}p^{1+(k-1)/3-1/3} & \text{if } (k-1)/2 \equiv 2 \pmod 3 \end{cases} \\ &= \frac{1}{\sqrt{1 - \left(\frac{D}{p}\right)\frac{1}{p}}} \begin{cases} p^{n/6} & \text{if } n \equiv 0 \pmod 3 \\ A_{\tilde{\alpha},1}p^{n/6-1/6} & \text{if } n \equiv 1 \pmod 3 \\ A_{\tilde{\alpha},2}p^{n/6-1/3} & \text{if } n \equiv 2 \pmod 3 \end{cases}, \end{aligned}$$

once again using Theorem 5.1. □

Let us also show that the "non-generic" newforms of a "generic" Hecke group have the same behavior for $N = p^n$, where $n = 2k + 1$ is odd, as we found for even n in [16]. In other words we study the case when $p|C$ and D is a square residue modulo p. Let $\sqrt{D}$ be an element in $\mathbb{Z}_N$ such that $\sqrt{D}^2 = D$ and define

$$V_\pm = \bigoplus_{\substack{x \in \mathbb{Z}_{p^{k+1}} \times \mathbb{Z}_{p^k} \\ x_1 \equiv \pm\sqrt{D}x_2 \not\equiv 0 \pmod p}} \mathbb{C}\zeta_{0,x}.$$

Proposition 5.4. *Let $N = p^n$ for some odd prime p and $n > 1$. Assume that $p|C$ and that D is a quadratic residue modulo p. If $\psi \in V_C \cap V_\pm$ is a normalized Hecke eigenfunction then*

$$|\psi(b)| = \begin{cases} \frac{1}{\sqrt{1-\frac{1}{p}}} & \textit{if } p \nmid b \\ 0 & \textit{if } p|b \end{cases}.$$

Proof. We can use the proof from [16], but we need to be careful. First of all we use the trick from Lemma 4.3 to write ψ as a sum of ψ_j and where all ψ_j have the same L^2-norm. Write ψ_j in the $\zeta_{0,x}-$basis and note that if the coefficients in front of $\zeta_{0,x}$ and $\zeta_{0,y}$ are nonzero, then $x \equiv y \pmod{p}$ by construction. Let $n = 2m+1$. The main step is to show that if $\zeta_{0,x}, \zeta_{0,y} \in V_C \cap V_+$ and $x \equiv y \pmod{p}$, then there exists an $h \in H_D$ such that $(hx)_1 \equiv y_1 \pmod{p^{m+1}}$, $(hx)_2 \equiv y_2 \pmod{p^m}$ and $T(h)0 = 0$. This is done by choosing $h_1 \equiv (y_1 - Dx_2h_2)x_1^{-1} \pmod{p^{m+1}}$ where h_2 is chosen so that $-Ch_2 \equiv x_1y_2 - x_2y_1 \pmod{p^m}$ and

$$\begin{vmatrix} h_1 & h_2D \\ h_2 & h_1 \end{vmatrix} \equiv 1 \pmod{N}.$$

For details of why such h_1 and h_2 exist and for the finishing observations, see the proof of Proposition 7.4 in [16]. The fact that $x \equiv y \pmod{p}$ implies that $h \equiv \mathrm{Id} \pmod{p}$ which gives $T(h)0 = 0$. □

The study done in [16] for the case when p is ramified can also be carried over to the case where N is an odd power of p. This is done in the same manner as we did in Theorem 5.2. We omit this and focus directly at the proof of Theorem 1.1 instead.

Proof of Theorem 1.1. To prove the theorem we need to prove that normalized Hecke eigenfunctions fulfill $\|\psi\|_\infty = O(N^{1/4})$ for all $N = p^n$, where p is not “bad”. However this is not quite enough because when we then want to use the tensor decomposition to get this estimate for all N the constants will make us lose too much. To handle this we also show that for all but a finite number of p the sharper estimate $\|\psi\|_\infty \leqslant N^{1/4}$ holds for $N = p^n$. Since this sharper estimate was proven in [16] for all odd p and even n, we assume that n is odd. That p is not “bad” means that $p \neq 2$, p is not ramified and A is not upper diagonal modulo p. Since we can not apply Theorem 5.3 to $p = 3$ we must treat this case separately. An easy calculation shows that $p = 3$ can not be split, hence if $p = 3$ is not “bad”, it is inert. By the observation that the value of a newform can be calculated as an exponential sum over the solutions to a quadratic equation modulo $[n/2]$ (or p such sums) we get $\|\psi\|_\infty = O(N^{1/4})$ for all newforms with $N = 3^n$ by using the trivial estimate of the exponential sum. Since $p = 3$ is inert, this gives us that $\|\psi\|_\infty = O(N^{1/4})$ for all Hecke eigenfunctions. For $p > 3$ we can use Theorem 5.2, Theorem 5.3 and Proposition 5.4 to get the estimate $\|\psi\|_\infty \leqslant 2N^{1/6}$ for all newforms and all but a finite number of p. When p is inert all Hecke eigenfunctions are newforms or the image of a newform by the unitary operator given in Theorem 3.1 and from this the two estimates we need follows, i.e., we get that $\|\psi\|_\infty \leqslant N^{1/4}$ for all but a finite number of p and $\|\psi\|_\infty = O(N^{1/4})$ for all p. When p is split things are a bit more complicated because a Hecke eigenfunction can be a sum of images of newforms. We let $l = [n/2]$ and write $\psi = a_0\psi_0 + a_1\psi_1 + ... + a_l\psi_l$, where $\psi_m \in S_n(n-m, m)$ but ψ_m is orthogonal to $S_n(n-m-1, m+1)$ and ψ_m is normalized. The key observation is now that by Proposition 5.4 the supports of ψ_i and ψ_j are disjoint if $i \neq j$. From this it follows also in the split case. □

Remark. Note that the estimate $\|\psi\|_\infty \leqslant N^{1/4}$ does not hold if $N = p^n$ where n is odd and p is small enough and split. Numerical simulations show that for $p \leqslant 13$ there are Hecke eigenfunctions with supremum norm larger than $p^{1/4}$.

6 Value distribution of newforms

In the introduction we described the limiting distribution of the absolute values of newforms as the image of the Haar measure of the normalizer of the maximal torus of $SU(2)$ under the map $g \mapsto |\operatorname{tr}(g)|$. More explicitly the measure is given by

$$\mu(f) = \frac{f(0)}{2} + \frac{1}{\pi}\int_0^2 \frac{f(x)}{\sqrt{4-x^2}}dx. \tag{13}$$

Since we have a well developed theory of evaluating newforms at different points, developed in Chapter 4 of this paper and Chapter 5 in [16], the limiting measure of a specific newform will follow almost immediately. From this theory it is also obvious that the assumption that $C_i \not\equiv C_j \pmod p$ is essential because there is a very strong correlation between the values of $\psi_{p,i}$ and $\psi_{p,j}$ otherwise. If we for instance assume that $\psi_{p,i}(x) = 0$ (true for approximately half of the points), the "probability" that $\psi_{p,j}(x) = 0$ converges to 1. Let us begin with the "immediate" part of our statement:

Proof of Theorem 1.2 and Theorem 1.3 for $d = 1$. The value $\psi(x)$ of $\psi \in V_C$ at a point $x \in \mathbb{Z}_{p^n}$ is a sum over the solutions to $y^2 \equiv -C + Dx^2 \pmod{p^{[n/2]}}$, where the absolute value of each term in the sum converges to 1 as $p \to \infty$. The number of solutions to the equation is at most two as long as $Dx^2 \not\equiv C \pmod p$ and the proportion of x where this is not true is $O(1/p)$. Thus the limiting measure is concentrated on $[0,2]$. To be a quadratic residue modulo $p^{[n/2]}$ is the same as being a quadratic residue modulo p and therefore we may restrict ourselves to calculating the proportion of x such that $-C + Dx^2$ is a quadratic residue modulo p. Note also that since D is fixed and p grows we may assume that $p \nmid D$. The total number of pairs (x, y) such that $y^2 - Dx^2 \equiv -C \pmod p$ is then (as we have seen a number of times before, for instance in the proof of Lemma 6.3 in [16])

$$p - \left(\frac{D}{p}\right).$$

Since all but at most 2 different x correspond to 2 different y we see that the proportion of x such that $-C+Dx^2$ is a quadratic residue converge to 1/2 and so does the proportion of x such that $-C+Dx^2$ is not a square. If $-C+Dx^2$ is not a square modulo p then obviously the value of $\psi(x)$ is zero and this corresponds to the first term of μ. On the other hand if $-C + Dx^2$ is equal to y^2 for some $y \not\equiv 0 \pmod p$, then we know that

$$\psi(x + tp^{[n/2]}) = a_+(x)e\left(\frac{yt}{p^{[n/2]}}\right) + a_-(x)e\left(\frac{-yt}{p^{[n/2]}}\right). \tag{14}$$

This might just as well be written as

$$\frac{\psi(x + tp^{[n/2]})}{a_+(x)e(y\alpha(x))} = \left[e\left(y\left(\frac{t}{p^{[n/2]}} - \alpha(x)\right)\right) + e\left(-y\left(\frac{t}{p^{[n/2]}} - \alpha(x)\right)\right)\right]$$

for $\alpha(x)$ given by $e(2y\alpha(x)) = a_-(x)/a_+(x)$. Averaging the absolute value of this as t goes through $\mathbb{Z}_{p^{[n/2]}}$ we see that the limit has the same value distribution as

$$\left|e^{i\theta} + e^{-i\theta}\right| = 2|\cos\theta|$$

there θ is uniform on the interval $0 \leqslant \theta < 2\pi$. This has the same value distribution as $2\cos\theta$ on the interval $0 \leqslant \theta \leqslant \pi/2$ and taking the derivative of the inverse of $2\cos\theta$ we get the second term in Equation (13). □

The independence will be established through some lemmas. The first lemma shows that the events $\psi_{p,1}(x) = 0, \psi_{p,2}(x) = 0, ..., \psi_{p,d}(x) = 0$ become statistically independent.

Lemma 6.1. *Let C_i be r different elements in $\mathbb{F}_p$ and let $M_r(p)$ denote the number of $x \in \mathbb{F}_p$ such that $-C_i + Dx^2$ is a square for all $i = 1, 2, ..., r$. Then*

$$M_r(p) = \frac{p}{2^r} + O_r(\sqrt{p}).$$

Proof. For all elements $x \in \mathbb{F}_p^\times$ we have that the expression

$$\frac{1 + \left(\frac{x}{p}\right)}{2}$$

is equal to 1 if x is a square and 0 if x is not a square. From this it follows that

$$\begin{aligned} M_r(p) &= \frac{1}{2^r} \sum_{x \in \mathbb{F}_p} \prod_{i=1}^{r} \left(1 + \left(\frac{-C + Dx^2}{p}\right)\right) + O_r(1) \\ &= \frac{1}{2^r} \sum_{x \in \mathbb{F}_p} 1 + \frac{1}{2^r} \sum_{i=1}^{r} \sum_{x \in \mathbb{F}_p} \left(\frac{-C_i + Dx^2}{p}\right) \\ &+ \frac{1}{2^r} \sum_{i \neq j} \sum_{x \in \mathbb{F}_p} \left(\frac{(-C_i + Dx^2)(-C_j + Dx^2)}{p}\right) \\ &+ ... + \frac{1}{2^r} \sum_{x \in \mathbb{F}_p} \left(\frac{\prod_{i=1}^{r}(-C_i + Dx^2)}{p}\right) + O_r(1). \end{aligned}$$

The first term gives the expression we want and and the other terms are bounded by $O_r(\sqrt{p})$ according to Theorem 2B in [18]. □

We will need the following lemma in the proof of Lemma 6.3:

Lemma 6.2. *Let $a \in \mathbb{F}_p^d$ be a non-zero vector and let C_i be different elements in $\mathbb{F}_p$ for $i = 1, ..., d$. Then the number of solutions in t and x to the system of equations*

$$\begin{cases} x_i^2 &= t - C_i \quad \textit{for all} \;\; i = 1, 2, ..., d \\ a \cdot x &= 0 \end{cases}$$

is uniformly bounded in p.

Proof. We fix an algebraically closed field extension $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$ and count the number of solutions there. Obviously this does not reduce the number of solutions. It is enough to show that the dimension of the solution set is zero, i.e. to prove that there are no two different closed (in the Zariski topology) irreducible subsets of the solution set such that $Z_0 \subset Z_1$. To prove such a statement it would be enough to show that the Jacobian of the system has full rank for all points in the solution set. However this is in general not true for our system of equations, but we will show that the number of points in the solution set such that the Jacobian does not have full rank is bounded. This means that the number of possible non-isolated points is bounded and from this it follows that the solution set itself is bounded.

If we put everything in the equations to the left and calculate the determinant of the Jacobian we get

$$J(x,t) = 2^{d-1} \sum_{k=1}^{d} a_k \prod_{j \neq k} x_j .$$

We want to prove that this is non-zero for all but a bounded number of points in the solution set. Let us now define $g(x,t)$ by

$$g(x,t) = \prod_{b \in \{-1,1\}^d} J(bx,t),$$

where $bx = (b_1x_1, b_2x_2, ..., b_dx_d)$. If we can prove that $g(x,t)$ has a bounded number of zeros in the solution set, then so does $J(x,t)$. Looking at our definition it is easy to see that $g(x,t)$ is an even polynomial in x, thus the restriction to the solution set (where $x_i^2 = t - C_i$) is a polynomial $h(t) \in \overline{\mathbb{F}_p}[t]$ in only the variable t. Polynomials in one variable have finite number of zeros as long as they are not the zero-polynomial, hence we only need to find one value of t such that $h(t) \neq 0$. Since $a \neq 0$ we know that $a_l \neq 0$ for some $l = 1, 2, ..., d$. If we put $t = C_l$ we see that $x_l = 0$ and that $x_j \neq 0$ for $j \neq l$, the latter because $C_j \neq C_l$. This shows that the factors $J(bx, C_l) = 2^{d-1} a_l \prod_{j \neq l} x_j \neq 0$ and since every factor is different from zero we must have $h(C_l) \neq 0$. A bounded number of solutions in t immediately gives a bounded number of solutions also in x. □

Remark. Our proof works for any field with characteristic different from two. From the boundedness it follows from Bezout's theorem that the number of solutions is at most 2^d, but we will only use that it is bounded.

The proof for $d = 1$ shows that the only values of x that can contribute to the left hand side of the expression in Theorem 1.2 are the ones where $y^2 \equiv -C_i + Dx^2 \pmod{p}$ has two or zero solutions for all $i = 1, ..., d$. Since this shows that the measure is concentrated on $[0,2]^d$ and any bounded continuous function can be uniformly approximated by polynomials on a compact set, we may assume that the test function f is a monomial. Let

$$\Omega_k(C_i) = \left\{ x \in \mathbb{Z}_{p^k} ; \left(\frac{-C_i + Dx^2}{p} \right) = 1 \right\} .$$

Hence Theorem 1.2 follows from:

Lemma 6.3. *Let $\psi_{p,j}$ and C_i be as in Theorem 1.2. Then for all sets of integers $m_j \geqslant 0$ we have*

$$\lim_{p \to \infty} \frac{1}{p^n} \sum_{x \in \bigcap_{i=1}^{d} \Omega_n(C_i)} \prod_{j=1}^{d} |\psi_{p,j}(x)|^{m_j} = \prod_{j=1}^{d} \left(\lim_{p \to \infty} \frac{1}{p^n} \sum_{x \in \Omega_n(C_j)} |\psi_{p,j}(x)|^{m_j} \right).$$

Proof. Let $k = [n/2]$ and $x_j^2 \equiv Dx^2 - C_j \pmod{p^k}$. In the proof for $n = 1$ we did not specify how we chose our a_+ and a_-, but now we have to be more careful.

Since we want to evaluate (14) for all $t \in \mathbb{Z}_{p^k}$ we may choose x (by adding $p^{\lceil n/2 \rceil}$ the appropriate number of times) to be such that $t \equiv 0 \pmod{p^{\lceil n/2 \rceil}}$ makes the absolute value as large as possible. In other words we choose x so that $|\arg(a_+/a_-)| \leqslant \pi/p^k$. This implies that

$$\left|\psi_{p,j}(x + tp^{\lceil n/2 \rceil})\right| = \left|1 + e\left(\frac{2x_j t}{p^k}\right)\right| + O\left(\frac{1}{p}\right),$$

hence it is enough to show that $|\phi_{p,j}|^2$, where $\phi_{p,j}$ are given by

$$\phi_{p,j}(x + tp^{\lceil n/2 \rceil}) = 1 + e\left(\frac{2x_j t}{p^k}\right),$$

become statistically independent. We do this by showing the equality in the lemma for $|\phi|^2$ instead of $|\psi|$. Since we take p to infinity we may assume that $p^k > m_j$ for all j. We may also assume that $m_j > 0$, since this only corresponds to changing d to be the number of non-zero m_j. The right hand side is now a product of d factors of the form

$$\begin{aligned}
\frac{1}{p^n} \sum_{x \in \Omega_n(C_j)} |\phi_{p,j}(x)|^{2m_j} &= \frac{1}{p^n} \sum_{x \in \Omega_{\lceil n/2 \rceil}(C_j)} \sum_{t \in \mathbb{Z}_{p^k}} \left(2 + e\left(\frac{2x_j t}{p^k}\right) + e\left(\frac{-2x_j t}{p^k}\right)\right)^{m_j} \\
&= \frac{1}{p^n} \sum_{x \in \Omega_{\lceil n/2 \rceil}(C_j)} \sum_{t \in \mathbb{Z}_{p^k}} \sum_{\substack{l_1, l_2 \geqslant 0; \\ l_1 + l_2 \leqslant m_j}} \binom{m_j}{m_j - l_1 - l_2, l_1, l_2} 2^{m_j - l_1 - l_2} e\left(\frac{2(l_1 - l_2)x_j t}{p^k}\right) \\
&= \frac{p^k}{p^n} \sum_{x \in \Omega_{\lceil n/2 \rceil}(C_j)} \sum_{l=0}^{[m_j/2]} \binom{m_j}{m_j - 2l, l, l} 2^{m_j - 2l},
\end{aligned}$$

where the last equality follows from $p \nmid 2x_j$ and $m_j < p^k$. Denote the inner sum by $f(m_j)$. Using Lemma 6.1 we see that the right hand side approaches $2^{-d} \prod_{j=1}^d f(m_j)$, as p goes to infinity. The same calculation for the left hand side shows that

$$\begin{aligned}
&\frac{1}{p^n} \sum_{x \in \bigcap_{i=1}^d \Omega_n(C_i)} \prod_{j=1}^d |\phi_{p,j}(x)|^{2m_j} \\
&\quad = \frac{1}{p^n} \sum_{x \in \bigcap_{i=1}^d \Omega_{\lceil n/2 \rceil}(C_i)} \sum_{t \in \mathbb{Z}_{p^k}} \prod_{j=1}^d \left(2 + e\left(\frac{2x_j t}{p^k}\right) + e\left(\frac{-2x_j t}{p^k}\right)\right)^{m_j} \\
&\quad = \frac{1}{p^n} \sum_{x \in \bigcap_{i=1}^d \Omega_{\lceil n/2 \rceil}(C_i)} \sum_{t \in \mathbb{Z}_{p^k}} \prod_{j=1}^d \sum_{\substack{l_{j,1}, l_{j,2} \geqslant 0; \\ l_{j,1} + l_{j,2} \leqslant m_j}} \binom{m_j}{m_j - l_{j,1} - l_{j,2}, l_{j,1}, l_{j,2}} \\
&\quad \times 2^{m_j - l_{j,1} - l_{j,2}} e\left(\frac{2(l_{j,1} - l_{j,2})x_j t}{p^k}\right).
\end{aligned}$$

If we calculate the product over the sums we get a large sum of expressions of the form

$$Ae\left(\frac{Bt}{p^k}\right),$$

where A is a product of multinomial coefficients and powers of 2 and B is the sum of $2(l_{j,1} - l_{j,2})x_j$, where $j = 1, 2, ..., d$. When we sum over t we get zero unless B is zero modulo p^k and by Lemma 6.2 we know that the number of x modulo p such that $B \equiv 0 \pmod{p^k}$ although $\{l_{j,1} - l_{j,2}\}_{j=1}^d \not\equiv 0$ is bounded for each such pair l_1, l_2. This shows that the number of $x \in \mathbb{Z}_{p^{\lceil n/2 \rceil}}$ such that $B \equiv 0 \pmod{p^k}$ is at most $O(p^{\lceil n/2 \rceil - 1})$. But there is a finite number of l, thus by Lemma 6.1 we have that

$$\begin{aligned}\frac{1}{p^n} \sum_{x \in \bigcap_{i=1}^d \Omega_n(C_i)} \prod_{j=1}^d |\phi_{p,j}(x)|^{2m_j} &= \lim_{p \to \infty} \frac{p^k}{p^n} \sum_{x \in \bigcap_{i=1}^d \Omega_{\lceil n/2 \rceil}(C_i)} \prod_{j=1}^d f(m_j) \\ &= \frac{1}{2^d} \prod_{j=1}^d f(m_j).\end{aligned}$$

□

6.1 Entropy of newforms

Let us discuss the consequences of Theorem 1.2 in terms of entropy:

Definition 6.1. Let $f \in L^2(\mathbb{Z}_N)$ and assume $\|f\|_2 = 1$. We define the Shannon entropy to be

$$h(f) = -\sum_{x \in \mathbb{Z}_N} \frac{|f(x)|^2}{N} \log \frac{|f(x)|^2}{N}.$$

It is known that the eigenfunctions of $U_N(A)$ fulfill $h(\psi) \geqslant 1/2 \log N$ (see Chapter 4 in [16]) and the trivial upper bound for all normalized functions is $h(\psi) \leqslant \log N$. There are no previous results on the entropy of newforms, but Corollary 1.4 shows that asymptotically this entropy is always maximal. Note that oldforms given by $T_m^{-1}\psi$, where ψ is a newform for a smaller power of p, asymptotically will have the Shannon entropy $\log p^{n-m}$. Recall that m can be any integer less or equal to $n/2$.

Proof of Corollary 1.4. Using equation (13) it is easy to check that $\mu(x^2) = 1 = \|\psi\|_2^2$. This is a small extension of Theorem 1.2 which shows that the estimate $|\psi(x)| \leqslant 2$ holds on a set X such that ψ restricted to X will have an L^2-norm which converges to 1. The contribution from points in X to the entropy is then at least $(1 - o(1)) \log(N/4)$, thus the Shannon entropy is asymptotically maximal. By Proposition 5.4 we see that the "non-generic" newforms also have maximal entropy. □

References

[1] R. Aurich, A. Bäcker, R. Schubert, and M. Taglieber. Maximum norms of chaotic quantum eigenstates and random waves. *Phys. D*, 129(1-2):1–14, 1999.

[2] R. Aurich and F. Steiner. Statistical properties of highly excited quantum eigenstates of a strongly chaotic system. *Phys. D*, 64(1-3):185–214, 1993.

[3] M. V. Berry. Regular and irregular semiclassical wavefunctions. *J. Phys. A*, 10(12):2083–2091, 1977.

[4] A. Bouzouina and S. De Bièvre. Equipartition of the eigenfunctions of quantized ergodic maps on the torus. *Comm. Math. Phys.*, 178(1):83–105, 1996.

[5] Mirko Degli Esposti. Quantization of the orientation preserving automorphisms of the torus. *Ann. Inst. H. Poincaré Phys. Théor.*, 58(3):323–341, 1993.

[6] Mirko Degli Esposti, Sandro Graffi, and Stefano Isola. Classical limit of the quantized hyperbolic toral automorphisms. *Comm. Math. Phys.*, 167(3):471–507, 1995.

[7] Frédéric Faure, Stéphane Nonnenmacher, and Stephan De Bièvre. Scarred eigenstates for quantum cat maps of minimal periods. *Comm. Math. Phys.*, 239(3):449–492, 2003.

[8] Dennis A. Hejhal and Barry N. Rackner. On the topography of Maass waveforms for $PSL(2, \mathbf{Z})$. *Experiment. Math.*, 1(4):275–305, 1992.

[9] H. Iwaniec and P. Sarnak. L^∞ norms of eigenfunctions of arithmetic surfaces. *Ann. of Math. (2)*, 141(2):301–320, 1995.

[10] Dubi Kelmer. On matrix elements for the quantized cat map modulo prime powers. *http://uk.arxiv.org/abs/0802.3237*.

[11] Stefan Knabe. On the quantisation of Arnold's cat. *J. Phys. A*, 23(11):2013–2025, 1990.

[12] Pär Kurlberg. Bounds on supremum norms for Hecke eigenfunctions of quantized cat maps. *Ann. Henri Poincaré*, 8(1):75–89, 2007.

[13] Pär Kurlberg and Zeév Rudnick. Hecke theory and equidistribution for the quantization of linear maps of the torus. *Duke Math. J.*, 103(1):47–77, 2000.

[14] Pär Kurlberg and Zeév Rudnick. Value distribution for eigenfunctions of desymmetrized quantum maps. *Internat. Math. Res. Notices*, (18):985–1002, 2001.

[15] Pär Kurlberg and Zeév Rudnick. On the distribution of matrix elements for the quantum cat map. *Ann. of Math. (2)*, 161(1):489–507, 2005.

[16] R. Olofsson. Large supremum norms and small Shannon entropy for Hecke eigenfunctions of quantized cat maps. *Comm. Math. Phys.*, 286(3):1051–1072, 2009.

[17] Peter Sarnak. Arithmetic quantum chaos. In *The Schur lectures (1992) (Tel Aviv)*, volume 8 of *Israel Math. Conf. Proc.*, pages 183–236. Bar-Ilan Univ., Ramat Gan, 1995.

[18] Wolfgang M. Schmidt. *Equations over finite fields. An elementary approach.* Springer-Verlag, Berlin, 1976. Lecture Notes in Mathematics, Vol. 536.

[19] Steven Zelditch. Index and dynamics of quantized contact transformations. *Ann. Inst. Fourier (Grenoble)*, 47(1):305–363, 1997.