MODULAR FORMS FOR $\Gamma_0(p)$

by

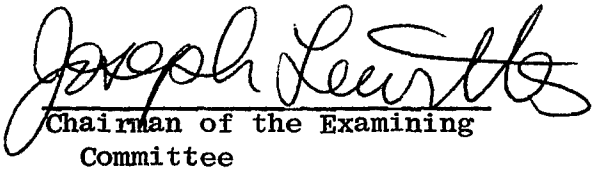
WALTER F. MODRYS, S.J.

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

1976

This manuscript has been read and accepted for the University Committee in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

April 26, 1976



Chairman of the Examining Committee

Professor Joseph Lewittes

April 26, 1976

Executive Officer
Professor Richard Sacksteder

Professor Harry E. Rauch

Professor Harvey Cohn

Supervisory Committee

ABSTRACT

MODULAR FORMS FOR $\Gamma_0(p)$

by

WALTER F. MODRYS, S.J.

Adviser: Professor Joseph Lewittes

From the theta series, functions of the form $\psi_f(\tau) = \sum_{n=0}^{\infty} p(n,f)e^{2\pi i n\tau}$ are obtained, where f is a binary quadratic form of discriminant $-p$ and $\rho(n,f)$ is the number of times the form f represents n. The product of any two such functions is an entire modular form of dimension -2 for $\Gamma_0(p)$ where $p \equiv 3(\text{mod } 4)$ and $p > 3$. Estimates are made on the dimension of the space spanned by such products. The function $E(\tau)$ in the space spanned by the Eisenstein Series of dimension -2 is also an entire modular form for $\Gamma_0(p)$. When $p \equiv 19(\text{mod } 24)$, E is not in the space spanned by the products of the ψ_f functions. When $p \equiv 23(\text{mod } 24)$ and $p > 311$, $i\infty$ is a Weierstrass point of $\Gamma_0^*(p) = \Gamma_0(p) \cup \Gamma_0(p)R$, where $R(\tau) = \frac{-1}{p\tau}$. When $p \equiv 3(\text{mod } 8)$, $h(-p)$ points, non-equivalent under $\Gamma_0(p)$, are found for which $\psi_f(\tau) = 0$ for every form f.

ACKNOWLEDGEMENT

AMDG

I would like to dedicate this dissertation to my parents.

I want to thank the many fellow Jesuits with whom I have lived during my years of graduate studies. Their understanding and encouragement were a never failing support.

It is customary to express some gratitude to one's dissertation director. In my case, I feel this is especially appropriate. What I can say here can never adequately express my debt of gratitude to Professor Joseph Lewittes. Suffice it to say that his own high standard of professional scholarship and personal concern will long be a constant source of inspiration to me. And for this I thank him.

The contribution of the students, faculty, and staff of the City University must be acknowledged. Though their dedication may seem routine to them, to the recipient it has always seemed extraordinary. Sophie Gerber, who typed this manuscript, is merely the most recent example that comes to mind. A sincere thanks to them all.

TABLE OF CONTENTS

INTRODUCTION

By means of specialized forms of the θ function, one is able to construct entire modular forms of dimension -2 for $\Gamma_0(p)$, when p is a prime congruent to 3 modulo 4. These functions do not in general span V, the space of entire modular forms of dimension -2 for $\Gamma_0(p)$. The question therefore emerges concerning the dimension of the subspace of V spanned by these θ functions.

In particular, Section 2 considers functions of the form

$$\psi_A(\tau) = \sum_{\alpha \in A} e^{2\pi i \tau N(\alpha)/L}$$

where A is an ideal in the ring of algebraic integers of $Q(\sqrt{-p})$, L is the norm of A, and τ is a variable with values in the upper half-plane. Such functions may also be expressed as

$$\psi_f(\tau) = \sum_{n=0}^{\infty} \rho(n,f)\, e^{2\pi i n \tau}$$

where f is a binary quadratic form of discriminant $-p$ corresponding to the ideal A and $\rho(n,f)$ is the number of times the form f represents n. The product of any two such functions determines an entire modular form of dimension -2. We denote the set of these products by $\Psi\Psi$ and the space they span over $\mathbb{C}$ by $\langle\Psi\Psi\rangle$.

In Section 3 we introduce the transformation $R: \tau \to -\frac{1}{p\tau}$ and construct a subspace, V_-, of V which contains each element of $\Psi\Psi$. V_- is the space of modular forms with eigenvalue -1 under the transformation R. The dimension of V_- is known.

Since properly equivalent quadratic forms and the corresponding opposite forms determine the same function, we obtain $H(-p)$ distinct

functions ψ_f which are also linearly independent, where $2H(-p) + 1 = h(-p)$ is the class number of $Q(\sqrt{-p})$. The total number of functions in the set $\Psi\Psi$ is therefore $\frac{(H+1)(H+2)}{2}$. The dimension of $\langle\Psi\Psi\rangle$ is thus bounded above by this value and by $\dim V_-$.

From the space of Eisenstein Series of dimension -2, we obtain (up to a multiplicative constant) exactly one entire modular form of dimension -2 for $\Gamma_0(p)$. This function, denoted by $E(\tau)$, is also contained in V_-.

In Section 4 it is shown that $E \notin \langle\Psi\Psi\rangle$ when p is congruent to 19 modulo 24. But there exist primes congruent to 7 modulo 8 for which $E \in \langle\Psi\Psi\rangle$ and other such primes for which $E \notin \langle\Psi\Psi\rangle$. Explicit primes are produced for which the functions in $\Psi\Psi$ neither span V_- nor are linearly independent. Such discussion involves the order of magnitude of $h(-p)$ when various conditions are imposed on p.

Tables listing the dimension of the space $\langle\Psi\Psi\rangle$ are presented for various primes congruent to 3 modulo 4 and less than 1000. These tables reveal that for such primes the dimension of $\langle\Psi\Psi\rangle$ actually equals the upper bound described above.

It is shown that, except for the first few primes, $i\infty$ is a Weierstrass point for $\Gamma_0^*(p)$, the group generated by $\Gamma_0(p)$ and R, when p is congruent to 23 modulo 24.

Finally, when p is congruent to 3 modulo 8, we are able to write down explicitly $h(-p)$ points in the upper half-plane that are non-equivalent under $\Gamma_0(p)$ and for which each ψ_f is zero at the point.

SECTION 1: PRELIMINARY REMARKS ON MODULAR FORMS, BINARY QUADRATIC FORMS AND IDEALS

(a) Modular Forms:

In this subsection we will summarize some results of the general theory of modular forms as expounded by Bruno Schoeneberg [10]. For purposes of notation, we adopt the convention that $\mathbb{Z}$ is the set of rational integers and $\mathbf{N}$ the positive integers. Q is the set of rational numbers, $\mathbb{R}$ the real numbers and $\mathbb{C}$ the complex numbers. $\mathfrak{H}$ is the upper half-plane; i.e., $\mathfrak{H} = \{\tau \in \mathbb{C}: \operatorname{Im} \tau > 0\}$, and $\mathfrak{H}^*$ is $\mathfrak{H}$ with the point $i\infty$ and the set Q adjoined. If a and b are in $\mathbb{Z}$, then $d = (a,b)$ means that d is the greatest common divisor of a and b.

The (full) modular group, Γ', is the set of two-by-two matrices with determinant 1 and integer entries. Γ' is generated by

$$S = \begin{pmatrix} 0 & -1 \\ +1 & 0 \end{pmatrix} \qquad \text{and} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} .$$

In the sequel, S and T will always denote these matrices (or their corresponding Mobius transformations). Γ' is homomorphic to Γ, the group of Mobius transformations. The homomorphism is simply

$$\varphi: \Gamma' \to \Gamma$$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \varphi A: \tau \to \frac{a\tau+b}{c\tau+d}$$

and has kernel $\pm I$, where I is the identity in Γ'. To simplify notation, when $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in Γ', we will frequently write $A(\tau)$ for the transformation $\varphi A: \tau \to \frac{a\tau+b}{c\tau+d}$.

Some of the subgroups of Γ' play leading roles in the theory of modular forms. For $N \geq 2$, $N \in \mathbf{N}$, we have the principal congruence

subgroup of level N, denoted in this paper by $\Gamma'_+(N)$. It is composed of those elements of Γ' of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a \equiv d \equiv 1 \pmod{N}$ and $c \equiv b \equiv 0 \pmod{N}$. A congruence subgroup of level N is a subgroup of Γ' which contains $\Gamma'_+(N)$. These terms are also applied to the corresponding subgroups in Γ. In particular, we have the congruence subgroup $\Gamma'_0(N)$, composed of those matrices of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $c \equiv 0 \pmod{N}$. We let $\Gamma_0(N)$ be the group of corresponding Mobius transformations; i.e., the image of $\Gamma'_0(N)$ under φ, The index of $\Gamma'_0(N)$ in Γ' is $N \prod_{\substack{q \mid N \\ q \text{ prime}}} (1 + \frac{1}{q})$. In particular, for p a prime, $\Gamma'_0(p)$ has index $p + 1$ in Γ'.

A fundamental domain of $\Gamma_0(p)$ may be chosen in such a way that there is one cusp at $i\infty$ of width 1 and another cusp at 0 of width p, and no other cusps. Under the usual identifications, $\mathcal{H}^*/\Gamma_0(p)$ forms a compact Riemann surface. The local coordinate at $i\infty$ is simply $\tau \to e^{2\pi i\tau}$, and that at 0 is $\tau \to e^{(2\pi i/p)\, S(\tau)}$. The genus, g, of the surface is given by:

$$g = \begin{cases} \dfrac{p-7}{12}, & \text{if } p \equiv 7 \pmod{12}, \text{ and} \\ \dfrac{p+1}{12}, & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

Let G be a subgroup of Γ of finite index. A point $\tau_0 \in \mathcal{H}$ is called an elliptic point of G if it is fixed by a transformation in G that is not the identity. Such a transformation is necessarily of order 2 or 3 and is called an elliptic transformation. If this order is 2, then τ_0 is Γ-equivalent to i; and if the order is 3, then τ_0 is Γ-equivalent to $\rho = e^{2\pi i/3}$. We let ϵ_i and ϵ_ρ be the number of

elliptic points of G in a fundamental domain of G that are Γ-equivalent to i or ρ, respectively. In particular, it can be shown that for $\Gamma_0(p)$ with p a prime greater than 3 we have

$$\epsilon_i = 1 + \left(\frac{-1}{p}\right),$$

and

$$\epsilon_\rho = 1 + \left(\frac{-3}{p}\right),$$

where the parentheses denote the Legendre symbol.

If f is a function on $\mathfrak{H}$ and $k \in \mathbb{Z}$, we adopt the notation

$$f|_{k,U}(\tau) = \frac{1}{(c\tau+d)^k} f(U(\tau))$$

where $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{R})$ and $U(\tau) = \frac{a\tau+b}{c\tau+d}$.

The definition of a modular form appears with some minor variations in the literature. To avoid confusion, we state

Definition: Let G be a subgroup of Γ' of finite index. The function f from $\mathfrak{H}$ into the extended complex plane is called a modular form for G of dimension $-k$ if

(i) f is meromorphic on $\mathfrak{H}$;

(ii) $f|_{k,U}(\tau) = f(\tau)$ for all $U \in G$;

(iii) Let w be the width of the cusp of G at $i\infty$, so that

$$\tau \to x = e^{\frac{2\pi i}{w}\tau}$$

is the local coordinate of $\mathfrak{H}^*/G$ at $i\infty$.

Then there exists an expansion of the form $f(\tau) = \sum_{\substack{n \geq N_{i\infty} \\ a_{N_{i\infty}} \neq 0}} a_n x^n$ for $\operatorname{Im} \tau$

sufficiently large.

(iv) Let w be the width of the cusp of G at $\gamma = -\frac{d}{c} \in \mathbb{Q}$, so that

$$\tau \to x = e^{\frac{2\pi i}{w} A(\tau)}$$

where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma'$ is the local coordinate of $\mathcal{H}^*/G$ at γ.

Then there exists an expansion of the form

$$(c\tau+d)^k f(\tau) = \sum_{\substack{n \geq N_\gamma \\ a_{N_\gamma} \neq 0}} a_n x^n$$

for $\operatorname{Im} A(\tau)$ sufficiently large.

In the light of this definition, $N_{i\infty}$ is called the order of f at $i\infty$ with respect to (w.r.t) the local coordinate, and N_γ is the order of f at γ w.r.t. the local coordinate. $i\infty$ or γ is a pole of f if $N_{i\infty} < 0$ or $N_\gamma < 0$, respectively.

It can be shown that for any $\tau_0 \in \mathcal{H}$ there exists an expansion of $(\tau-\bar{\tau}_0)^k f(\tau)$ in terms of the local coordinate at τ_0. Using this expansion, we define the order of f at τ_0 w.r.t. the local coordinate in the obvious manner. If τ_0 is a regular (non-elliptic) point, this order coincides with the order of f at τ_0 determined by its Laurent series. If τ_0 is elliptic and fixed by a transformation in G of order j, then j times the order of f (w.r.t. the local coordinate) equals the order determined by the Laurent series of f. It can be shown that the orders of f at G-equivalent points are the same. These facts are used to prove the result that in a fundamental domain for G, the number of zeros of f minus the number of poles (w.r.t. the local coordinates) must equal $\frac{k\mu}{12}$, where μ is the index of $G \cup (-I)G$ in Γ'.

The modular form f is called <u>entire</u> if it has no poles. Applying this theory to $\Gamma_0'(p)$ where p is prime, we see that an entire modular form of dimension -2 for $\Gamma_0'(p)$ has $\frac{p+1}{6}$ zeros in a fundamental domain, since $p+1$ is the index.

The entire modular forms for G of dimension $-k$ span a vector space, V, over $\mathbb{C}$. If $k \geq 2$, the Riemann-Roch Theorem can be used to obtain its dimension:

$$\dim V = (k-1)(g-1) + \left[\frac{k}{4}\right]\epsilon_i + \left[\frac{k}{3}\right]\epsilon_p + \frac{k}{2}\sigma_\infty ,$$

where g is the genus of $\mathfrak{H}^*/G$, and σ_∞ is the number of cusps in a fundamental domain for G. $\left[\frac{k}{4}\right]$ is the largest integer in $\frac{k}{4}$, and similarly for $\left[\frac{k}{3}\right]$. In particular, when $k = 2$, $\dim V = g + \sigma_\infty - 1$. We see that for $\Gamma_0'(p)$ and $k = 2$, $\dim V = g+1$, since $\Gamma_0(p)$ has two cusps.

The importance of modular forms of dimension $-k$ lies in the fact that they determine differentials on the surface, at least when k is even. In particular, an entire modular form, f, of dimension -2 determines a differential $\omega = f(\tau)d\tau$ that is analytic everywhere except possibly at the cusps. Using the notation in our previous definition,

$$\omega(x) = \frac{w}{2\pi i} \sum_{\substack{n \geq N_{i\infty} \\ a_{N_{i\infty}} \neq 0}} a_n x^{n-1}$$

is the expansion of $\omega = f(\tau)d\tau$ at $i\infty$. Thus, ω is analytic at $i\infty$ if $N_{i\infty} > 0$, and ω has a simple pole at $i\infty$ with residue $\frac{w}{2\pi i} a_0$ if $N_{i\infty} = 0$. Similarly for the finite cusps. We see then that if f is a cusp form of dimension -2, that is, if f is entire and has a zero at each cusp, then the corresponding differential $\omega = f(\tau)d\tau$

is of the 1^{st} kind. If f is entire but not a cusp form, then $\omega = f(\tau)d\tau$ is of the 3^{rd} kind.

In later secions we will construct explicitly entire modular forms of dimension -2 for $\Gamma_0'(p)$ when $p \equiv 3 \pmod 4$. We will then examine the dimension of the subspace of V spanned by these modular forms. The calculation of this dimension will involve some facts concerning the representation of numbers by binary quadratic forms, to which we now turn our attention.

(b) Binary Quadratic Forms

In this subsection, the word "form" generally will refer to a binary quadratic form. Throughout this paper, in order to avoid confusion, a modular form is never referred to simply as a "form". The results listed in this subsection can be found in Dickson [3].

A binary quadratic form is an expression of the form $f(x,y) = ax^2 + bxy + cy^2$, where $a,b,c \in \mathbb{Z}$. The form is primitive if g.c.d. $\{a,b,c\} = 1$. The discriminant, $D(f)$, of f is $b^2 - 4ac$. Two forms, $f_1(x,y) = a_1x^2 + b_1xy + c_1y^2$ (abbreviated as $f = [a_1,b_1,c_1]$) and $f_2 = [a_2,b_2,c_2]$ are called properly equivalent if there exists some element $U = \begin{pmatrix} \alpha & \beta \\ \gamma & d \end{pmatrix} \in \Gamma'$ such that

$$f_1(\alpha x + \beta y, \gamma x + \delta y) = f_2(x,y) .$$

For convenience, we will write this relation in the form $f_1 U\begin{pmatrix} x \\ y \end{pmatrix} = f_2\begin{pmatrix} x \\ y \end{pmatrix}$. The form opposite to $f = [a,b,c]$ is $f' = [a,-b,c]$. The form f is positive-definite if $f(x,y)$ is positive except when $x = y = 0$. This is equivalent to $D(f) < 0$ and $a > 0$. It can be shown that every primitive, positive-definite form of given discriminant

is properly equivalent to precisely one reduced form of that discriminant. A form $f = [a,b,c]$ is reduced if $-a < b \leq a$, $c \geq a$, and $b \geq 0$ whenever $c = a$. If p is a prime and $p \equiv 3 \pmod 4$, $p > 3$, then $f_0 = [1,1,\frac{p+1}{4}]$ is called the principal form of discriminant $-p$ and is reduced. Furthermore, all other reduced forms of discriminant $-p$ are of the form $f = [a,b,c]$ with $1 \leq b < a < c$, and the opposite forms, $f' = [a,-b,c]$.

From now on, p will always denote a prime greater than 3 such that $p \equiv 3 \pmod 4$.

If $f = [a,b,c]$ is reduced with $D(f) = -p$, then $1 \leq a < \sqrt{p/3}$, $\frac{3}{4}\sqrt{p/3} < c$, and $a - b + c > \sqrt{p/3}$. For, $4a^2 < 4ac = b^2 + p \leq a^2 + p$, which implies $3a^2 < p$. Hence, $c = \frac{b^2+p}{4a} > \frac{b^2+p}{4\sqrt{p/3}} \geq \frac{1}{4}\frac{1+p}{\sqrt{p/3}} = \frac{3}{4}\frac{1+p}{p}\sqrt{p/3}$ $> \frac{3}{4}\sqrt{p/3}$. Furthermore,

$$a-b+c = \frac{1}{4a}[4a^2-4ab+4ac] = \frac{1}{4a}[(2a-b)^2+p] \geq \frac{1}{4a}[a^2+p] = \frac{1}{4}[a+\frac{p}{a}] > \sqrt{p/3}\ .$$

This implies in particular that the total number of reduced forms is finite. Thus, a complete set of non-equivalent reduced forms of discriminant $-p$ is given by:

$$f_0 = \left[1,1,\frac{p+1}{4}\right]$$

$$f_1 = [a_1,b_1,c_1] \qquad \text{and} \qquad f' = [a_1,-b_1,c_1]$$

$$\vdots \qquad\qquad\qquad\qquad \vdots$$

$$f_H = [a_H,b_H,c_H] \qquad\qquad f'_H = [a_H,-b_H,c_H]$$

where $1 \leq b_j < a_j < c_j$ for $1 \leq j \leq H$. We let $h(-p)$ denote the number of forms in this complete set, so that $h(-p) = 2H+1$. This notation will be used frequently in the sequel.

Of course, $h(-p)$ is the class number of the field $K = Q(\sqrt{-p})$.

This notion will be discussed in the following subsection. For now, we mention only that $h(-p)$ is finite and an odd integer. Also, as a function of p, $h(-p)$ varies with a high degree of irregularity. However, Dirichlet proved the famous result that

$$h(-p) = \begin{cases} \sum_{r=1}^{\frac{p-1}{2}} \left(\frac{r}{p}\right), & \text{if } p \equiv 7 \pmod 8 \\ \frac{1}{3} \sum_{r=1}^{\frac{p-1}{2}} \left(\frac{r}{p}\right), & \text{if } p \equiv 3 \pmod 8,\ p > 3 . \end{cases}$$

We will be interested in the number of times a given number is represented by a given form; that is, in the number, $\rho(n,f)$, of integral solutions x,y of $f(x,y) = n$. Since all forms in our discussion are positive-definite, $\rho(n,f) = 0$ if $n < 0$ and $\rho(0,f) = 1$. Clearly, properly equivalent forms represent the same numbers, each the same number of times. The same holds for any form and its opposite. We let $\rho(n,p)$ be the total number of representations of n by a maximal set of non-equivalent forms of discriminant $-p$. We will make frequent use of the standard results concerning the representability of numbers by forms. For convenience, we list some of these results. All forms are assumed to be positive-definite of discriminant $-p$ where $p \equiv 3 \pmod 4$ and $p > 3$.

Proposition 1: If $m \in \mathbf{N}$ and $(m,p) = 1$, let

$$m = \prod_{\substack{q \mid m \\ q \text{ prime}}} q^{v_q(m)}$$

be the prime factorization of m. That is, $v_q(m)$ is the exponent to which the prime q enters in m. If

$$m_+ = \prod_{\substack{q \mid m \\ \left(\frac{q}{p}\right)=1}} q^{v_q(m)} \qquad \text{and} \qquad m_- = \prod_{\substack{q \mid m \\ \left(\frac{q}{p}\right)=-1}} q^{v_q(m)}$$

then

$$\rho(m,p) = \begin{cases} 2D(m_+) , & \text{if } m_- \text{ is a perfect square, and} \\ 0 , & \text{otherwise} \end{cases}$$

$D(m_+)$ is the number of positive divisors of m_+ .

The proof follows from the result that $\rho(m,p) = 2 \sum_{\substack{d>0 \\ d \mid m}} \left(\frac{-p}{d}\right)$.

([3], pg. 78.)

On the other hand, if $m = np^j \in \mathbf{N}$ where $(n,p) = 1$, then we have $\rho(m,p) = \rho(n,p)$. This well-known result will follow easily from the results of Section 2.

The following proposition is helpful for later calculations:

Proposition 2: Let $f = [a,b,c]$, $b > 0$, be reduced. Then:

(i) If $t = \min\{|x|, |y|\}$, then $f(x,y) \begin{cases} = t^2(a-b+c), & \text{if } x = -y; \text{ and} \\ > t^2(a-b+c), & \text{otherwise .} \end{cases}$

(ii) If f is non-principal and $m \in \mathbf{N}$, then $0 < m \leq \max\{c, \sqrt{p/3}\}$ implies $\rho(m,f) = \begin{cases} 2, & \text{if } m = ax^2 \text{ or } m = c; \text{ and} \\ 0, & \text{otherwise.} \end{cases}$

(iii) If f is principal and $m \in \mathbf{N}$, then $0 < m \leq \frac{p+1}{4}$ implies

$$\rho(m,f) = \begin{cases} 4, & \text{if } m = \frac{p+1}{4} \\ 2, & \text{if } m = x^2 , \text{ and} \\ 0, & \text{otherwise.} \end{cases}$$

It is also true that if $f = [a,b,c]$ is reduced and $a' > 0$ divides a, then there exists some form $[a',b',c']$ that is also reduced.

(c) Ideals

The results of this subsection can be found in [1] and [2].

We assume that p is a prime, $p > 3$, and $p \equiv 3 \pmod 4$. If $f = [a,b,c]$ is a positive-definite binary quadratic form of discriminant $-p$, then by factoring $ax^2 + bxy + cy^2$ we can obtain

$$f(x,y) = \frac{\left|ax + \left(\frac{b+1}{2} - \omega\right) y\right|^2}{a}$$

where $\omega = \frac{1+\sqrt{-p}}{2}$. This fact leads to the correspondence between forms and ideals.

In general, the quadratic field $K = Q(\sqrt{-p})$ has I_K for its ring of algebraic integers, where $I_K = \mathbb{Z} + \mathbb{Z}\omega$ and $\omega = \frac{1+\sqrt{-p}}{2}$ (since we have $p \equiv 3 \pmod 4$). An additive subgroup of I_K is called a <u>module</u>, and the module is <u>full</u> if it is generated by two linearly independent elements. A full module M is therefore generated by two linearly independent elements, α and β, and we write $M = [\alpha,\beta] = \{x\alpha + y\beta: x,y \in \mathbb{Z}\}$. The basis α,β is said to be ordered if

$$\frac{1}{\sqrt{-p}} \det \begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix} > 0 ,$$

where $\bar{\alpha}$ and $\bar{\beta}$ denote the complex conjugates of α and β, respectively. If $M = [\alpha,\beta]$ and α,β is not ordered, then clearly $M = [\beta,\alpha]$ is an ordered basis. A full module M may also be an ideal in I_K. This means that $\gamma M \subseteq M$ for all $\gamma \in I_K$.

The opening remarks of this subsection show that we may associate the form $f = [a,b,c]$ with the full module $M = [a, \frac{b+1}{2} - \omega]$ where the <u>norm</u> of M, $N(M)$, equals a. In fact, M is also an ideal of I_K.

Adopting the usual notation, $N(z) = |z|^2$, we can write

$$f(x,y) = \frac{N\left(ax + \left(\frac{b+1}{2} - \omega\right) y\right)}{N(M)}$$

where $M = [a, \frac{b+1}{2} - \omega]$ is an ideal in I_K with the ordered basis $[a, \frac{b+1}{2} - \omega]$.

Conversely, any ideal M that has, as a module, the ordered basis $[\alpha,\beta]$ determines the positive-definite form f of discriminant $-p$ given by

$$(*) \quad f(x,y) = \frac{N(x\alpha + y\beta)}{N(M)} = ax^2 + bxy + cy^2 .$$

Here $a = \frac{N(\alpha)}{N(M)}$, $b = \frac{Tr(\alpha\bar{\beta})}{N(M)}$, and $c = \frac{N(\beta)}{N(M)}$. $Tr(z)$ is the <u>trace</u> of z and equals $z + \bar{z}$.

We see from (*) that when the form f corresponds to the ideal M, we then have

$$\rho(n,f) = \left|\left\{\mu \in M: \frac{N(\mu)}{N(M)} = n\right\}\right| ,$$

where $|\{\}|$ denotes the cardinal number of the set.

We note that since $f = [a,b,c]$ corresponds to the ideal $M = [a, \frac{b+1}{2} - \omega]$, the opposite form $f' = [a,-b,c]$ must correspond to the conjugate ideal $\bar{M}$ with ordered basis $[-a, \frac{b+1}{2} - \bar{\omega}]$. Also, the principal form corresponds to $I_K = [1,\omega]$.

We have already defined the relation of proper equivalence between forms. This relation is of course an equivalence relation. We also define an equivalence relation on the set of non-zero ideals of I_K . The non-zero ideals M_1 and M_2 of I_K are said to be <u>similar</u> if $\alpha M_1 = \beta M_2$ for some non-zero $\alpha,\beta \in I_K$. With this definition, one can define a one-to-one correspondence between the equivalence classes of

ideals in I_K and the equivalence classes of positive-definite forms of discriminant $-p$. In particular, one can show that each equivalence class of ideals contains exactly one ideal with the ordered basis $[a, \frac{b+1}{2} - \omega]$ corresponding to the reduced form $f = [a,b,c]$.

The equivalence classes of ideals in I_K are called the <u>classes</u> of K. The number of classes is called the <u>class number</u> of K and denoted by $h(-p)$. The classes form a finite group of order $h(-p)$. The identity element of the group is the class determined by the principal ideals.

An ideal P in I_K is called a <u>prime ideal</u> if whenever M_1 and M_2 are ideals in I_K with $M_1M_2 \subseteq P$, then either $M_1 \subseteq P$ or $M_2 \subseteq P$. An important fact of the theory of ideals is that every ideal can be uniquely expressed as the product of prime ideals.

SECTION 2. MODULAR FORMS FOR $\Gamma_0'(p)$

Our main reference in this section is the Lewittes' paper [8]. That paper investigates how the θ function of several variables transforms under a general element of the modular group. In this section we will apply these results in order to obtain modular forms for $\Gamma_0'(p)$. The special theta functions we study have been chosen not only with this purpose in mind, but also to facilitate by means of quadratic forms the calculation of the dimension of the space spanned by such functions.

Let $K = Q(\sqrt{d})$ be an imaginary quadratic field with A a module in K of norm $N(A) = L$. For $x,y,z \in \mathbb{C}$ and $\tau \in \mathcal{H}$, we define the theta series

$$(1) \qquad \theta_A\left[\begin{matrix} x \\ y \end{matrix}\right](z,\tau) = \sum_{\alpha \in A} e^{2\pi i \, Tr(\alpha+x)(z+y) + 2\pi i \tau N(\alpha+x)} \, .$$

Here $Tr(z)$ is the trace $z+\bar{z}$; and $N(z)$ is the norm $z\bar{z}$, where $\bar{z}$ is the complex conjugate of z. x and y are called the characteristics. The series in (1) is absolutely and uniformly convergent in the variables z and τ on compact subsets of $\mathbb{C} \times \mathcal{H}$. For convenience, we set $\theta_A\left[\begin{matrix} x \\ y \end{matrix}\right](0,\tau) = \theta_A\left[\begin{matrix} x \\ y \end{matrix}\right](\tau)$. Later formulas will simplify if instead of θ_A we consider

$$(2) \qquad \psi_A\left[\begin{matrix} x \\ y \end{matrix}\right](\tau) = \theta_A\left[\begin{matrix} x \\ y \end{matrix}\right]\left(\frac{\tau}{L}\right) = \sum_{\alpha \in A} e^{2\pi i \, Tr(\alpha+x)y + 2\pi i \tau \frac{N(\alpha+x)}{L}} \, .$$

We first note that the functions defined with respect to similar modules differ merely in the characteristics. That is, if $\beta \in K$, then

$$(3) \qquad \psi_{\beta A}\left[\begin{matrix} x \\ y \end{matrix}\right](\tau) = \psi_A\left[\begin{matrix} \beta^{-1} x \\ \beta \quad y \end{matrix}\right](\tau) \, .$$

Furthermore,

$$(4) \qquad \psi_{\bar{A}}\begin{bmatrix} x \\ y \end{bmatrix}(\tau) = \psi_A\begin{bmatrix} \bar{x} \\ \bar{y} \end{bmatrix}(\tau) \ .$$

To derive modular forms for $\Gamma_0'(p)$ from the functions defined by (2), it is helpful to impose the following conditions. First, we take K to be the quadratic field $K = Q(\sqrt{-p})$, where as always p denotes a prime greater than 3 and $p \equiv 3 \pmod 4$. Secondly, we assume that the upper characteristic is in $\frac{1}{\sqrt{-p}} A$, where A is assumed to be a full module in I_K and also an ideal of I_K. Finally we set the lower characteristic equal to 0. Under these conditions, the most important transformation formula for our purposes simplifies to:

$$(5) \qquad M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_0'(p) \quad \text{and} \quad x \in A \quad \text{implies}$$

$$\psi_A\begin{bmatrix} x/\sqrt{-p} \\ 0 \end{bmatrix}\Big|_{1,M}(\tau) = e^{2\pi i \frac{\alpha\beta}{L} N(x/\sqrt{-p})} \left(\frac{\delta}{p}\right) \psi_A\begin{bmatrix} \alpha x/\sqrt{-p} \\ 0 \end{bmatrix}(\tau)$$

where $\left(\frac{\delta}{p}\right)$ denotes the Legendre symbol.

On the other hand, if $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma' - \Gamma_0'(p)$, it is shown in [8] that for $x \in A$,

$$(6) \qquad \psi_A\begin{bmatrix} x/\sqrt{-p} \\ 0 \end{bmatrix}\Big|_{1,M}(\tau) = e^{-2\pi i \frac{\alpha\beta}{L} N(x/\sqrt{-p})} \left(\frac{\gamma}{p}\right) 1/\sqrt{-p}$$

$$\sum_{k \pmod p} e^{2\pi i \gamma^* \delta\, k^2 L/p} \psi_A\begin{bmatrix} (\alpha x + kL)/\sqrt{-p} \\ -\beta\bar{x}/L\sqrt{-p} \end{bmatrix}(\tau)$$

where γ^* satisfies $\gamma\gamma^* \equiv 1 \pmod p$.

From (5) we see that setting x equal to 0 yields a modular

form of dimension -1 with a multiplier. We will later show that the square of such a function is in fact a modular form for $\Gamma_0'(p)$ of dimension -2. But first we examine the expansion of the function $\psi_A\begin{bmatrix} x/\sqrt{-p} \\ 0 \end{bmatrix}(\tau)$ using (2).

Because of (3) and (4) we lose no generality in assuming that the module A has the basis $\{a, \frac{b+1}{2} - \omega\}$ where $a = N(A) = L$, $b \in \mathbf{N}$, and $\omega = \frac{1+\sqrt{-p}}{2}$. Thus, as in Section 1(c), A corresponds to the reduced form $f = [a,b,c]$ of discriminant -p. The expansion of $\psi_A\begin{bmatrix} 0 \\ 0 \end{bmatrix}(\tau)$ then becomes by (2):

$$\psi_A\begin{bmatrix} 0 \\ 0 \end{bmatrix}(\tau) = \sum_{\alpha \in A} e^{2\pi i \tau N(\alpha)/L} .$$

But if $\alpha = n_1 a + n_2\left(\frac{b+1}{2} - \omega\right)$, then $N(\alpha) = af(n_1,n_2)$ where $a = L$. So

$$\psi_A\begin{bmatrix} 0 \\ 0 \end{bmatrix}(\tau) = \sum_{n_1,n_2 \in \mathbf{Z}} e^{2\pi i \tau f(n_1,n_2)} .$$

Letting $\rho(n,f)$ be the number of times the form f represents n, we obtain

$$\psi_A\begin{bmatrix} 0 \\ 0 \end{bmatrix}(\tau) = \sum_{n=0}^{\infty} \rho(n,f)\, e^{2\pi i n \tau} . \tag{7}$$

We next seek to obtain a similar expansion for $\psi_A\begin{bmatrix} x/\sqrt{-p} \\ 0 \end{bmatrix}(\tau)$ when $x \in A$ but $x \neq 0$. From (2) we have

$$\psi_A\begin{bmatrix} x/\sqrt{-p} \\ 0 \end{bmatrix}(\tau) = \sum_{\alpha \in A} e^{2\pi i \tau \frac{N(\alpha+(x/\sqrt{-p}))}{L}} = \sum_{\alpha \in A} e^{\frac{2\pi i}{p} \tau \frac{N(\alpha\sqrt{-p}+x)}{L}} . \tag{8}$$

In order to introduce the binary form f corresponding to A into this expansion, we employ the fact that $\frac{1}{\sqrt{-p}} A/A$ is a cyclic group

of order p generated by $A + L/\sqrt{-p}$. That is

$$\frac{1}{\sqrt{-p}} A = \bigcup_{t(\mathrm{mod}\ p)} \left(A + \frac{Lt}{\sqrt{-p}}\right),$$

so that $A = \bigcup_{t(\mathrm{mod}\ p)} (A\sqrt{-p} + Lt)$. This fact is proved in [8]. Letting x equal Lj where j is fixed and $(j,p) = 1$ will introduce the form f into the expansion because of the following lemma.

The symbol $|\{\ \}|$ denotes the cardinal number of the set.

Lemma: For $j \not\equiv 0(\mathrm{mod}\ p)$ and $n \geq 0$,

$$\left|\left\{\alpha \in A: \frac{N(\sqrt{-p}\alpha + Lj)}{L} = n\right\}\right| = \begin{cases} \frac{1}{2}\rho(n,f), & \text{if } n \equiv Lj^2(\mathrm{mod}\ p) \\ 0, & \text{otherwise} \end{cases}$$

Proof: Let β be an element in $A = \bigcup_{t(\mathrm{mod}\ p)} (A\sqrt{-p} + Lt)$. Then for some $n_1, n_2 \in \mathbb{Z}$ and for some $t_0 \in \{0,1,\ldots,p-1\}$,

$$\beta = \left[n_1 L + n_2\left(\frac{b+1}{2} - \omega\right)\right]\sqrt{-p} + Lt_0 .$$

Hence,

$$\frac{N(\beta)}{L} = pf(n_1,n_2) + n_2 t_0 p + Lt_0^2 .$$

If $\beta \in A\sqrt{-p} + Lj$ so that t_0 equals j, then clearly $\frac{N(\beta)}{L} \equiv Lj^2(\mathrm{mod}\ p)$. Conversely, if $\frac{N(\beta)}{L} \equiv Lj^2(\mathrm{mod}\ p)$, then $t_0^2 \equiv j^2(\mathrm{mod}\ p)$, so that $\beta \in (A\sqrt{-p} + Lj) \cup (A\sqrt{-p} - Lj)$. Therefore, if $n \equiv Lj^2(\mathrm{mod}\ p)$, we have

$$\begin{aligned} \left|\left\{\beta \in A: \frac{N(\beta)}{L} = n\right\}\right| &= \left|\left\{\beta \in A\sqrt{-p} + Lj: \frac{N(\beta)}{L} = n\right\}\right| + \left|\left\{\beta \in A\sqrt{-p} - Lj: \frac{N(\beta)}{L} = n\right\}\right| \\ &= \left|\left\{\alpha \in A: \frac{N(\alpha\sqrt{-p} + Lj)}{L} = n\right\}\right| + \left|\left\{\alpha \in A: \frac{N(\alpha\sqrt{-p} - Lj)}{L} = n\right\}\right| \\ &= 2\left|\left\{\alpha \in A: \frac{N(\alpha\sqrt{-p} + Lj)}{L} = n\right\}\right| . \end{aligned}$$

But since $\left|\left\{\beta \in A: \frac{N(\beta)}{L} = n\right\}\right|$ is simply $\rho(n,f)$, the Lemma follows.

Returning to (8), we set x equal to Lj where $j \not\equiv 0 \pmod p$. Using the Lemma, we argue as in the derivation of (7) and obtain:

$$(9) \quad \psi_A \begin{bmatrix} Lj/\sqrt{-p} \\ 0 \end{bmatrix} (\tau) = \tfrac{1}{2} \sum_{\substack{n=0 \\ n \equiv Lj^2 \pmod p}}^{\infty} \rho(n,f)\, e^{\frac{2\pi i}{p} n\tau}$$

To simplify notation, we now define:

$$\psi_{f,j}(\tau) = \psi_A \begin{bmatrix} Lj/\sqrt{-p} \\ 0 \end{bmatrix} (\tau)$$

where A corresponds to $f = [a,b,c]$, a reduced form of discriminant $-p$. The two functions $\psi_{f,j_1}(\tau)$ and $\psi_{f,j_2}(\tau)$ are identical if $j_1 \equiv j_2 \pmod p$. We also write $\psi_f(\tau)$ for $\psi_{f,0}(\tau)$.

The transformation formulas (5) and (6) may now be re-written. With the substitution of Lj for x, where $j \in \{0,1,\ldots,p-1\}$, we have:

$$(10) \quad M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_0'(p) \text{ implies } \psi_{f,j}\big|_{1,M}(\tau) = e^{\frac{2\pi i}{p} \alpha\beta Lj^2} \left(\frac{\delta}{p}\right) \psi_{f,\alpha j}(\tau) .$$

Similarly, (6) yields: $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma' - \Gamma_0'(p)$ and $\gamma\gamma^* \equiv 1 \pmod p$ implies

$$\psi_A \begin{bmatrix} Lj/\sqrt{-p} \\ 0 \end{bmatrix}\Big|_{1,M} (\tau) = e^{\frac{-2\pi i}{p} \alpha\beta Lj^2} \left(\frac{\gamma}{p}\right) \frac{1}{\sqrt{-p}} \sum_{k \pmod p} e^{\frac{2\pi i}{p} \gamma^* \delta Lk^2} \psi_A \begin{bmatrix} (\alpha j+k)L/\sqrt{-p} \\ -\beta j/\sqrt{-p} \end{bmatrix} (\tau).$$

However,

$$\psi_A \begin{bmatrix} (\alpha j+k)\ L/\sqrt{-p} \\ -\beta j/\sqrt{-p} \end{bmatrix} (\tau) = e^{\frac{2\pi i}{p} \cdot 2L\beta j(\alpha j+k)} \psi_A \begin{bmatrix} L(\alpha j+k)/\sqrt{-p} \\ 0 \end{bmatrix} (\tau) ,$$

so that

$$\psi_A\left[\begin{matrix} Lj/\sqrt{-p} \\ 0 \end{matrix}\right]\Big|_{1,M}(\tau) = e^{\frac{2\pi i}{p} L\alpha\beta j^2}\left(\frac{\gamma}{p}\right)\frac{1}{\sqrt{-p}} \sum_{k(\mathrm{mod}\ p)} e^{\frac{2\pi i}{p}L(k-\alpha j)[\gamma^*\delta(k-\alpha j)+2\beta j]}\psi_A\left[\begin{matrix} Lk/\sqrt{-p} \\ 0 \end{matrix}\right](\tau) .$$

Finally, we have

$$(11)\qquad \psi_{f,j}\Big|_{1,M}(\tau) = e^{\frac{2\pi i}{p}\alpha\beta L j^2}\left(\frac{\gamma}{p}\right)\frac{1}{\sqrt{-p}} \sum_{k(\mathrm{mod}\ p)} e^{\frac{2\pi i}{p}L(k-\alpha j)[\gamma^*\delta(k-\alpha j)+2\beta j]}\psi_{f,k}(\tau) .$$

Of special importance for the construction of modular forms for $\Gamma_0'(p)$ is equation (11) when $S = \left(\begin{matrix} 0 & -1 \\ 1 & 0 \end{matrix}\right)$ is substituted for M. For later reference, we have:

$$(12)\qquad \psi_{f,j}\Big|_{1,S}(\tau) = \frac{1}{\sqrt{-p}} \sum_{k(\mathrm{mod}\ p)} e^{\frac{2\pi i}{p}(-2Ljk)}\psi_{f,k}(\tau) .$$

In particular, for $j \equiv 0 (\mathrm{mod}\ p)$, we obtain:

$$(13)\qquad \psi_f\Big|_{1,S}(\tau) = \frac{1}{\sqrt{-p}}\psi_f\left(\frac{\tau}{p}\right) .$$

This last formula is derived merely by expanding the summation in (12) and recalling that $A = \bigcup_{t(\mathrm{mod}\ p)} (\sqrt{-p}\,A + Lt)$. We add the remark that from (12) and (13) easily follows the well-known fact that for $j \in \mathbb{Z}$, $\rho(jp,f) = \rho(j,f)$. To see this, we have from (12),

$$\psi_f\Big|_{1,S}(\tau) = \frac{1}{\sqrt{-p}}\left\{\sum_{\substack{n=0\\ n\equiv 0(\mathrm{mpd}\ p)}}^{\infty} \rho\left(\frac{n}{p},f\right)e^{\frac{2\pi i}{p}n\tau} + \sum_{\substack{n=0\\ n\not\equiv 0(\mathrm{mod}\ p)}}^{\infty} \rho(n,f)e^{\frac{2\pi i}{p}n\tau}\right\}.$$

On the other hand, from (13),

$$\psi_f\Big|_{1,S}(\tau) = \frac{1}{\sqrt{-p}}\sum_{n=0}^{\infty}\rho(n,f)\,e^{\frac{2\pi i}{p}n\tau}.$$

Thus, $n \equiv 0(\mathrm{mod}\ p)$ implies $\rho\left(\frac{n}{p},f\right) = \rho(n,f)$.

For the convenience of the reader we list the main formulas thus far in our discussion. The numbers in parentheses are those previously assigned to the respective formulas in the text.

I. A a module in $K = Q(\sqrt{d})$ of norm L; $x,y \in \mathbb{C}$.

(2) $$\psi_A\left[\begin{matrix}x\\ y\end{matrix}\right](\tau) = \sum_{\alpha\in A} e^{2\pi i\,\mathbf{Tr}(\alpha+x)y+2\pi i\tau\frac{N(\alpha+x)}{L}}$$

II. A a full module in I_K, $K = Q(\sqrt{-p})$, and an ideal in I_K; $N(A) = L$.

A corresponds to $f = [a,b,c]$; $a = L$.

(7) $$\psi_f(\tau) = \psi_A\left[\begin{matrix}0\\ 0\end{matrix}\right](\tau) = \sum_{\alpha\in A} e^{2\pi i\tau\frac{N(\alpha)}{L}} = \sum_{n=0}^{\infty}\rho(n,f)e^{2\pi i n\tau}$$

(9) $j \not\equiv 0(\mathrm{mod}\ p)$

$$\psi_{f,j}(\tau) = \psi_A\left[\begin{matrix}-Lj/\sqrt{-p}\\ 0\end{matrix}\right](\tau) = \sum_{\alpha\in A} e^{\frac{2\pi i}{p}\tau\frac{N(\alpha\sqrt{-p}+Lj)}{L}} = \tfrac{1}{2}\sum_{\substack{n=0\\ n\equiv Lj^2(\mathrm{mod}\ p)}}^{\infty}\rho(n,f)e^{\frac{2\pi i}{p}n\tau}$$

(10) $M = \left(\begin{matrix}\alpha & \beta\\ \gamma & \delta\end{matrix}\right) \in \Gamma_0'(p)$ implies $\psi_{f,j}\Big|_{1,M}(\tau) = e^{\frac{2\pi i}{p}\alpha\beta Lj^2}\left(\frac{\delta}{p}\right)\psi_{f,\alpha j}(\tau)$

(11) $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma' - \Gamma_0'(p)$, $\gamma^*\gamma \equiv 1 \pmod p$ implies

$$\psi_{f,j}\Big|_{1,M}(\tau) = e^{\frac{2\pi i}{p}\alpha\beta Lj^2}\left(\frac{\gamma}{p}\right)\frac{1}{\sqrt{-p}}\sum_{k \pmod p} e^{\frac{2\pi i}{p}L(k-\alpha j)[\gamma^*\delta(k-\alpha j)+2\beta j]}\psi_{f,k}(\tau).$$

$$(12)\quad \psi_{f,j}\Big|_{1,S}(\tau) = \frac{1}{\sqrt{-p}}\sum_{k \pmod p} e^{-\frac{2\pi i}{p}\cdot 2Ljk}\psi_{f,k}(\tau)$$

$$(13)\quad \psi_f\Big|_{1,S}(\tau) = \frac{1}{\sqrt{-p}}\,\psi_f\left(\frac{\tau}{p}\right)$$

We are now in a position to prove the principal result of this section. That is, we can write down explicitly functions which are entire modular forms of dimension -2 for $\Gamma_0'(p)$.

Proposition: If f_1 and f_2 are reduced forms of discriminant $-p$, then the product $\psi_{f_1}\psi_{f_2}$ is an entire modular form for $\Gamma_0'(p)$ of dimension -2 with the expansions

$$\psi_{f_1}\psi_{f_2}(\tau) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\rho(n-k,f_1)\,\rho(k,f_2)\right)e^{2\pi i n\tau} \quad \text{at } i\infty$$

$$\tau^2\psi_{f_1}\psi_{f_2}(\tau) = -\frac{1}{p}\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\rho(n-k,f_1)\,\rho(k,f_2)\right)e^{\frac{2\pi i}{p}nS(\tau)} \quad \text{at } 0 .$$

We remark that the notation f_1 and f_2 above is used to indicate binary quadratic forms, so that $\psi_{f_1}(\tau)$ means $\psi_{f_1,0}(\tau)$. f_1 and f_2 are not necessarily distinct.

Proof: By (10), the product $\psi_{f_1}\psi_{f_2}$ satisfies the required transformation equation. The expansion at $i\infty$ follows from equation (7).

For the expansion at 0, the local coordinate at 0 is $e^{\frac{2\pi i}{p}z}$ where $z = S(\tau)$. We obtain from (13):

$$\left(\psi_{f_1}\psi_{f_2}\right)\Big|_{2,S}(z) = \psi_{f_1}\Big|_{1,S}(z) \cdot \psi_{f_2}\Big|_{1,S}(z) = \frac{1}{\sqrt{-p}}\psi_{f_1}\left(\frac{z}{p}\right) \cdot \frac{1}{\sqrt{-p}}\psi_{f_2}\left(\frac{z}{p}\right) .$$

That is,

$$\frac{1}{z^2}\psi_{f_1}\psi_{f_2}(Sz) = -\frac{1}{p}\psi_{f_1}\psi_{f_2}\left(\frac{z}{p}\right) .$$

So

$$\tau^2\psi_{f_1}\psi_{f_2}(\tau) = -\frac{1}{p}\psi_{f_1}\psi_{f_2}\left(\frac{S(\tau)}{p}\right) ,$$

and the proof is complete.

It is clear from (10) that each $\psi_{f,j}(\tau)$ is an entire modular form of dimension -2 for $\Gamma'_+(p)$, where $\Gamma'_+(p)$ is the principal congruence subgroup of level p as defined in Section 1. This suggests that we can form a sum of products of the ψ functions over a set of cosets of $\Gamma'_+(p)$ and generate additional modular forms of dimension -2 for $\Gamma'_0(p)$. That is, letting

$$\Gamma'_0(p) = \bigcup_{k=1}^{p(p-1)} \Gamma'_+(p)A_k$$

where each A_k is of the form

$$\begin{pmatrix} a + \ell p & \ell a^* + \frac{aa^*-1}{p} \\ p & a^* \end{pmatrix}$$

for $1 \le a, a^* \le p-1$, $aa^* \equiv 1 \pmod p$, and $0 \le \ell \le p-1$, we form

$$\psi_{f,j_1;f,j_2;\Gamma_0(p)}(\tau) = \sum_{k=1}^{p(p-1)} \psi_{f,j_1}\Big|_{1,A_k}(\tau) \cdot \psi_{f,j_2}\Big|_{1,A_k}(\tau) .$$

This function is then an entire modular form of dimension -2 for $\Gamma'_0(p)$. However, it is identically zero, except for $j_1 \equiv j_2 \equiv 0 \pmod p$,

in which case we merely obtain $p(p-1)\psi_{f_1}\psi_{f_2}$. Therefore, for the rest of our discussion, we will confine our attention to ψ functions with $0,0$ characteristics. Hence, the index j in ψ_{f_j} will in the sequel always refer to the quadratic form f_j, and not to the characteristics of the function.

Eisenstein Series of dimension -2 were originally introduced by Hecke. When the above argument is employed with the Eisenstein Series of dimension -2 and level p in place of the ψ functions, we obtain a non-zero modular form of dimension -2 for $\Gamma_0'(p)$. Furthermore, since $\Gamma_0(p)$ has exactly two cusps, there is (up to a multiplicative constant) exactly one entire modular form of dimension -2 in the space spanned by the Eisenstein Series of dimension -2 and level p ([10], p. 173). We alter Schoeneberg's notation slightly and write such a function as

$$E(\tau) = E(\tau,p) = \frac{p-1}{24} + \sum_{n=1}^{\infty} \Big(\sum_{\substack{d>0 \\ d\,|\,n \\ (p,d)=1}} d \Big) e^{2\pi i n \tau} . \tag{14}$$

We have

$$M \in \Gamma_0'(p) \quad \text{implies} \quad E\big|_{2,M}(\tau) = E(\tau) \tag{15}$$

and

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{implies} \quad E\big|_{2,S}(\tau) = -\frac{1}{p} E\Big(\frac{\tau}{p}\Big) . \tag{16}$$

(16) can be shown by writing $E(\tau)$ as a linear combination of Eisenstein Series and applying the transformation S to each term in the sum.

SECTION 3: THE SUBSPACE V_-

In Section 2 we have written down explicitly functions which are entire modular forms for $\Gamma_0'(p)$. On the one hand, we have seen that the reduced binary quadratic forms f_1 and f_2 (not necessarily distinct) of discriminant $-p$ determine the modular form $\psi_{f_1}\psi_{f_2}(\tau)$. On the other hand, we know that $E(\tau)$ in the space of Eisenstein series of dimension -2 is also a modular form for $\Gamma_0'(p)$.

For convenience, we introduce the following notation. Let $\Psi = \{\psi_f(\tau): f = [a,b,c]$ reduced, $b > 0$, $D(f) = -p\}$. We let $\langle\Psi\rangle$ be the vector space over $\mathbb{C}$ spanned by the functions in the set Ψ. $\Psi\Psi$ is the set of functions formed by the products of any two functions in Ψ. There are $H+1$ functions in Ψ where $2H+1 = h(-p)$ is the class number of $Q(\sqrt{-p})$. Hence, the number of functions in $\Psi\Psi$ is $\frac{(H+1)(H+2)}{2}$. $\langle\Psi\Psi\rangle$ denotes the space spanned by the functions in $\Psi\Psi$, and $\langle\Psi\Psi,E\rangle$ is the space spanned by the functions in $\Psi\Psi \cup \{E\}$.

The results of Section 2 imply that $\langle\Psi\Psi\rangle$ and $\langle\Psi\Psi,E\rangle$ are subspaces of V, where again V is the space of entire modular forms for $\Gamma_0'(p)$ of dimension -2. For what values of p does $\langle\Psi\Psi\rangle$ equal $\langle\Psi\Psi,E\rangle$? When are there linear relations between the functions in $\Psi\Psi$? What is the dimension of $\langle\Psi\Psi\rangle$?

In [5] Hecke writes down the explicit linear relations between the functions in $\Psi\Psi$ and E for the primes 23, 31, and 47. For 23 and 31 there are only three functions in $\Psi\Psi$, and for 47 there are only six functions, so that the calculations are relatively easy. But for $p = 719$, we already have 136 functions in $\Psi\Psi$, so that a straightforward calculation of the desired relations is quite difficult.

Hecke does not address the general problem.

In this section, we will begin to provide at least a partial answer to some of the above questions. Our starting point is the definition of a subspace, V_-, of V where V_- will contain $\langle \Psi\Psi, E\rangle$. Since the dimension of V_- is known, we therefore obtain an upper limit for $\dim\langle \Psi\Psi, E\rangle$, and so also for $\dim\langle \Psi\Psi\rangle$. In later sections, these considerations will involve estimates on $h(-p)$.

We consider the matrix $R = \begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & 0 \end{pmatrix}$ in $SL(2,\mathbb{R})$. $R^2 = -I$ and R determines the transformation $\tau \to -1/p\tau$ taking $\mathcal{H}^*$ onto itself. R is in the normalizer (w.r.t. $SL(2,\mathbb{R})$) of $\Gamma_0'(p)$. If $\Gamma_0^*(p) = \langle \Gamma_0'(p), R\rangle$, the subgroup of $SL(2,\mathbb{R})$ generated by $\Gamma_0'(p)$ and R, then clearly $\Gamma_0^*(p) = \Gamma_0'(p) \cup \Gamma_0'(p)R$. The transformation R also determines the analytic involution R^* on $\mathcal{H}^*/\Gamma_0(p)$ taking $\langle\tau\rangle$ into $\langle R(\tau)\rangle$.

The transformation formulas for R are:

$$\psi_f\Big|_{1,R}(\tau) = -i\psi_f(\tau) \quad \text{for } \psi_f \in \Psi \tag{17}$$

$$E\Big|_{2,R}(\tau) = -E(\tau) \tag{18}$$

(17) follows from the fact that

$$\psi_f\Big|_{1,R}(\tau) = \frac{1}{\sqrt{p}\tau}\,\psi_f\left(-\frac{1}{p\tau}\right) = \sqrt{p}\,\psi_f\Big|_{1,S}(p\tau) = -i\psi_f(\tau) \quad \text{by (13).}$$

(18) follows in a similar fashion from (16). Also, (17) implies

(19) $$\psi_{f_1}\psi_{f_2}\Big|_{2,R}(\tau) = -\psi_{f_1}\psi_{f_2}(\tau), \quad \text{for } \psi_{f_1}\psi_{f_2} \in \Psi\Psi .$$

For $f \in V$, the map $f \to f\Big|_{2,R}$ is a non-singular linear transformation of V into V with eigenvalues $+1$ and -1. Hence $V = V_+ \oplus V_-$ where $V_+ = \{f \in V: f\Big|_{2,R} = f\}$ and $V_- = \{f \in V: f\Big|_{2,R} = -f\}$.

From (18) and (19), we see that $\langle \Psi\Psi, E\rangle$ is a subspace of V_-.

Since $V = V_+ \oplus V_-$ and $\dim V = g + 1$, where g is the genus of $\mathcal{S} = \mathcal{H}^*/\Gamma_0(p)$, we have

(20) $$\dim V_- = g + 1 - \dim V_+ .$$

By identifying points in $\mathcal{H}^*$ under $\Gamma_0^*(p)$, we obtain a Riemann surface $\mathcal{S}^* = \mathcal{H}^*/\Gamma_0^*(p)$ of genus $g^* = g^*(p)$. g^* is equal to the dimension of the space spanned by the abelian differentials on $\mathcal{S}^*$ of the 1^{st} kind ([12], p. 253). Since $\mathcal{S}^*$ is $\mathcal{S}/\langle R\rangle$, the quotient space of the surface $\mathcal{S} = \mathcal{H}^*/\Gamma_0(p)$ under the group of automorphisms generated by R, we know that the abelian differentials of 1^{st} kind for $\mathcal{S}^*$ are precisely the abelian differentials of 1^{st} kind for $\mathcal{S}$ that are also invariant under R. That is, if $\omega = f(\tau)d\tau$ determines an abelian differential of 1^{st} kind for $\mathcal{S}^*$, then by Section 1(a) we must have $f \notin V_0$ and also $f \in V_+$, where V_0 is the space of cusp forms in V. Therefore, $g^* = \dim(V_+ \cap V_0)$.

Furthermore, $V_+ \subseteq V_0$. To see this, let $f \notin V_+$. Then we also have $f \notin V$. As in Section 1(a), we may write the expansions:

$$f(z) = \sum_{n=0}^{\infty} a_n x_\infty^n , \quad x_\infty = e^{2\pi i z} , \quad \text{at } i\infty .$$

$$\tau^2 f(\tau) = \sum_{n=0}^{\infty} b_n x_0^n \ , \ x_0 = e^{\frac{2\pi i}{p} S(\tau)} \ , \text{ at } 0 \ .$$

The abelian differential on $\mathcal{H}^*/\Gamma_0(p)$ given by $\omega = f(\tau)d\tau$ is analytic in $\mathcal{H}$ and has (at most) simple poles at $i\infty$ and 0 with residues $\frac{1}{2\pi i} a_0$ at $i\infty$ and $p \frac{1}{2\pi i} b_0$ at 0. But on a compact Riemann surface the sum of the residues of an abelian differential is zero. Therefore, $a_0 + pb_0 = 0$ and $a_0 = -pb_0$.

On the other hand, since $f \in V_+$, we also have $f|_{2,R}(\tau) = f(\tau)$, so that $f(z) = p\tau^2 f(\tau)$ where $z = R(\tau)$. Hence, using the above expansions, for $\operatorname{Im} z$ sufficiently large, so that $\operatorname{Im} S(\tau)$ is also large, we have:

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z} = \sum_{n=0}^{\infty} a_n e^{2\pi i n(-1/p\tau)} = \sum_{n=0}^{\infty} a_n e^{\frac{2\pi i}{p} n S(\tau)} \ ,$$

and

$$p\tau^2 f(\tau) = p \sum_{n=0}^{\infty} b_n e^{\frac{2\pi i}{p} n S(\tau)} \ .$$

Now $f(z) = p\tau^2 f(\tau)$ implies $a_n = pb_n$, so in particular $a_0 = pb_0$. Thus, $a_0 = pb_0 = -pb_0$, so $b_0 = a_0 = 0$ and f is a cusp form. I.e., $f \in V_0$.

Since $V_+ \subseteq V_0$, we have $g^* = \dim(V_+ \cap V_0) = \dim V_+$. This result along with (20) now yields

$$\dim V_- = g + 1 - g^* \ . \tag{21}$$

The genus, g^*, of $\mathcal{S}^*$ has been calculated by Fricke and is given in [7] by:

$$g(p) - 2g^*(p) = -1 + \tfrac{1}{2} \delta_p h(-4p) \ ,$$

where

$$\delta_p = \begin{cases} 2, & \text{if} \quad p \not\equiv 7 \pmod 8 \\ \frac{4}{3}, & \text{if} \quad p \equiv 3 \pmod 8 \\ 1, & \text{otherwise.} \end{cases}$$

It is known that

$$h(-4p) = \begin{cases} h(-p), & \text{if} \quad p \equiv 7 \pmod 8 \\ 3h(-p), & \text{if} \quad p \equiv 3 \pmod 8 \ . \end{cases}$$

We therefore obtain:

$$(22) \qquad g^* = g^*(p) = \begin{cases} \frac{p+5}{24} - \frac{1}{2}h(-p), & \text{if} \quad p \equiv 7 \pmod{24} \\ \frac{p+13}{24} - h(-p), & \text{if} \quad p \equiv 11 \pmod{24} \\ \frac{p+5}{24} - h(-p), & \text{if} \quad p \equiv 19 \pmod{24} \\ \frac{p+13}{24} - \frac{1}{2}h(-p), & \text{if} \quad p \equiv 23 \pmod{24} . \end{cases}$$

Using (21) and (22) and the notation $h(-p) = 2H+1$, we obtain:

$$(23) \qquad \dim V_- = \begin{cases} \frac{p-7}{24} + H+1, & \text{if} \quad p \equiv 7 \pmod{24} \\ \frac{p+13}{24} + 2H+1, & \text{if} \quad p \equiv 11 \pmod{24} \\ \frac{p+5}{24} + 2H+1, & \text{if} \quad p \equiv 19 \pmod{24} \\ \frac{p+1}{24} + H+1, & \text{if} \quad p \equiv 23 \pmod{24} \ . \end{cases}$$

From (18) and (19) we have $E \in V_-$ and $\langle \Psi\Psi \rangle$ a subspace of V_-. Thus, $\dim\langle \Psi\Psi, E \rangle \leq \dim V_-$. Furthermore, $\dim\langle \Psi\Psi \rangle \leq \frac{(H+1)(H+2)}{2}$, the total number of functions in $\Psi\Psi$. Therefore

$$(24) \qquad \dim\langle \Psi\Psi \rangle \leq \min \left\{ \frac{(H+1)(H+2)}{2}, \dim V_- \right\} \ .$$

We will show that $2H+1$ is a lower bound for $\dim\langle \Psi\Psi \rangle$. Unfortunately, this lower bound is too small to be of much service in the

actual calculation of $\dim\langle\Psi\Psi\rangle$ for particular values of p, except for some trivial cases. In any event, the result follows from

Proposition: $\dim\langle\Psi\rangle = H+1$. That is, the functions $\psi_f \in \Psi$ are linearly independent.

Proof: The proof proceeds in two steps. First, we show that each form represents a prime. The elements of the argument can be found in [2]. Secondly, we show that this implies the linear independence of the functions in Ψ .

In Section 2, we have shown that for any reduced form f, $n \equiv 0 \pmod p$ implies $\rho(\frac{n}{p}, f) = \rho(n,f)$. When $f = f_0$, the principal form, we let $n = p$ and obtain

$$\rho(p,f_0) = \rho(\tfrac{p}{p}, f_0) = \rho(1,f_0) = 2 .$$

In particular, we have $f_0(-1,2) = f_0(1,-2) = p$.

To show that every positive-definite form of discriminant $-p$ represents some prime q, we require more general considerations concerning the ideals of I_K , the ring of algebraic integers of $K = Q(\sqrt{-p})$.

Choose a form f. Then the equivalence class of forms determined by f corresponds to some ideal class $\mathcal{C}$ in I_K . By a theorem originally proved by Weber, each class contains an infinite number of prime ideals. We let P be a prime ideal in $\mathcal{C}$, where P corresponds to the form g, a form properly equivalent to f. f and g thus represent the same numbers. By the general theory, P contains a rational prime q . We let (q) denote the Ideal of I_K generated by q. If $q = p$, then $(p) = P^2$ and $N(P) = p$. Since $p \in P$, $g(x,y) = \frac{N(p)}{N(P)} = p$ for some $x,y \in \mathbb{Z}$ and g is necessarily

properly equivalent to the principal form. If $\left(\frac{q}{p}\right) = -1$, where $\left(\frac{q}{p}\right)$ is the Legendre symbol, then $(q) = P$, so that P is similar to the ideal $(1) = I_K$, which implies that the form g is properly equivalent to the principal form. Therefore g, and so also f, represents the prime p. On the other hand, if $\left(\frac{q}{p}\right) = 1$, then $(q) = P\bar{P}$ where $\bar{P}$ is the ideal conjugate to P, and $N(P) = q$. We let $P = [\alpha, \beta]$ so that there exist $x,y \in \mathbb{Z}$ such that $x\alpha + y\beta = q$. Then

$$g(x,y) = \frac{N(x\alpha + y\beta)}{N(P)} = \frac{N(q)}{q} = q .$$

Therefore g, and so also f, represents the prime q.

For the second part of the proof, let $\{f_0, f_1, \ldots, f_H\}$ be the set of reduced forms which determine the elements $\psi_f \in \Psi$ where f_0 is the principal form. Say f_j, $j \geq 1$, represents the prime q_j. By Section 1(b), q_j is represented twice by f_j and twice by the opposite form f_j', and by no other form. Then

$$F(\tau) = \sum_{j=0}^{H} A_j \psi_{f_j}(\tau) = \sum_{j=0}^{H} A_j \sum_{n=0}^{\infty} \rho(n, f_j) x^n$$

$$= \sum_{n=0}^{\infty} \left\{ \sum_{j=0}^{H} A_j \rho(n, f_j) \right\} x^n , \text{ where } x = e^{2\pi i \tau} .$$

Therefore, the coefficient of the q_j^{th} term of F is $2A_j$ for $1 \leq j \leq H$. Furthermore, since f_0 represents p, the coefficient of the p^{th} term of F is $2A_0$. Thus, F is identically zero if, and only if, each $A_j = 0$ for $0 \leq j \leq H$. So the functions ψ_{f_j}, $0 \leq j \leq H$, are linearly independent.

In general, given any finite set $\Psi = \{\psi_1, \ldots, \psi_K\}$ of convergent-power series in x, by forming linear combinations we may form a basis $\{\varphi_1, \ldots, \varphi_J\}$ for the space $\langle\Psi\rangle$ spanned by the set Ψ so that N_j is

the order of φ_j and $N_1 < N_2 < \ldots < N_J$. The set of N_j's so obtained is unique and may be denoted $ORD\langle\Psi\rangle$. Clearly, $|ORD\langle\Psi\rangle|$, the cardinal number of $ORD\langle\Psi\rangle$, equals $\dim\langle\Psi\rangle$. The space $\langle\Psi\Psi\rangle$ generated by the products of any two elements of Ψ contains a function whose order is given by $N_j + N_\ell$. We define $d\langle\Psi\Psi\rangle$ to be the set of integers formed by the elements of $ORD\langle\Psi\rangle$ added two at a time. Since $N_1+N_1 < N_1+N_2 < \ldots < N_1+N_J < N_2+N_J < \ldots < N_J+N_J$, we see that $d\langle\Psi\Psi\rangle$ has at least $2J-1$ distinct elements. Furthermore, $d\langle\Psi\Psi\rangle$ is a subset of $ORD\langle\Psi\Psi\rangle$. Therefore,

$$2J-1 \leq |d\langle\Psi\Psi\rangle| \leq |ORD\langle\Psi\Psi\rangle|.$$

Thus, $2\dim\langle\Psi\rangle - 1 \leq \dim\langle\Psi\Psi\rangle$.

We now apply these general notions to the functions

$$\psi_f(\tau) = 1 + \sum_{n=0}^{\infty} \rho(n,f)x^n$$

where $x = e^{2\pi i\tau}$. By the previous proposition, $\dim\langle\Psi\rangle = H+1$, so that $2H+1 = 2\dim\langle\Psi\rangle - 1 \leq \dim\langle\Psi\Psi\rangle$. The main result of this section is expressed in the following

Theorem: $$2H+1 \leq \dim\langle\Psi\Psi\rangle \leq \min\left\{\frac{(H+1)(H+2)}{2},\ \dim V_-\right\}$$

where $h(-p) = 2H+1$ and $\dim V_-$ is given by (23).

The general notions advanced above also frequently facilitate the actual computation of $\dim\langle\Psi\Psi\rangle$. For example, when $p = 239$, we have the reduced forms (with $b > 0$):

$f_0 = [1,1,60]$ $\qquad$ $f_4 = [5,1,12]$
$f_1 = [2,1,30]$ $\qquad$ $f_5 = [6,1,10]$
$f_2 = [3,1,20]$ $\qquad$ $f_6 = [6,5,11]$
$f_3 = [4,1,15]$ $\qquad$ $f_7 = [8,7,9]$

Letting $\varphi_0(\tau) = \psi_{f_7}(\tau)$ and $\varphi_j(\tau) = \psi_{f_j}(\tau) - \psi_{f_{j+1}}(\tau)$, $0 \le j \le 6$, we obtain $ORD\langle\Psi\rangle = \{0,1,2,3,4,5,6,10\}$. For $d\langle\Psi\Psi\rangle$ we have $\{0,1,\ldots,16,20\}$. Then $18 = |d\langle\Psi\Psi\rangle| \le \dim\langle\Psi\Psi\rangle \le \dim V_- = 18$, so that $\dim\langle\Psi\Psi\rangle = 18$.

It is true that each $N \in ORD\langle\Psi\rangle$ has $N \le \frac{p+1}{24}$. For, if $F(\tau) = \sum_{j=0}^{H} A_j \psi_{f_j}(\tau) = \sum_{n \ge N} a_n x^n$, $a_N \neq 0$, $x = e^{2\pi i\tau}$, then $F^2(\tau)$ is an entire modular form of dim -2 for $\Gamma_0'(p)$. $F^2(\tau) = a_N^2 x^{2N} + \ldots$ is the expansion at $i\infty$ and

$$\tau^2 F^2(\tau) = -\frac{1}{p}\left\{a_N^2 x^{2N} + \ldots\right\}, \quad x = e^{\frac{2\pi i}{p}S(\tau)}$$

is the expansion at 0. Therefore, $2N + 2N \le \frac{2(p+1)}{12}$, the total number of zeros of F^2 in $\mathcal{H}^*/\Gamma_0(p)$. That is, $N \le \frac{p+1}{24}$.

The questions posed at the beginning of this section can now be addressed in the light of the above theorem. For example, if for a particular value of p, we have $\frac{(H+1)(H+2)}{2} > \dim V_-$, then the functions in $\Psi\Psi$ cannot be linearly independent. On the other hand, if $\frac{(H+1)(H+2)}{2} < \dim V_-$, then the functions in $\Psi\Psi$ do not span V_-. These considerations lead to investigations of the order of magnitude of $h(-p)$.

An examination of the case for some primes less than 1000 leads to the conjecture that $\dim\langle\Psi\Psi\rangle = \min\left\{\frac{(H+1)(H+2)}{2}, \dim V_-\right\}$. Is this true in general? The next section will consider this question.

Since the formula (23) for $\dim V_-$ varies according to the residue class of p modulo 24, it is convenient to consider separately the cases for p(mod 24). Since we always have assumed $p \equiv 3 \pmod 4$ and $p > 3$, we have $p \equiv 7, 11, 19,$ or $23 \pmod{24}$. For later reference, we list:

$p \equiv 7 \pmod{24}$ implies $\left(\frac{2}{p}\right) = 1$, $\left(\frac{3}{p}\right) = -1$.

$p \equiv 11 \pmod{24}$ implies $\left(\frac{2}{p}\right) = -1$, $\left(\frac{3}{p}\right) = 1$.

$p \equiv 19 \pmod{24}$ implies $\left(\frac{2}{p}\right) = -1$, $\left(\frac{3}{p}\right) = -1$.

$p \equiv 23 \pmod{24}$ implies $\left(\frac{2}{p}\right) = 1$, $\left(\frac{3}{p}\right) = 1$.

SECTION 4: DIMENSION OF $\langle\Psi\Psi\rangle$, WEIERSTRASS POINTS AND ZEROS

(a) $\dim\langle\Psi\Psi\rangle$ and $\dim\langle\Psi\Psi,E\rangle$.

Frequent reference is made in this subsection to the table [9] which was obtained from the Unpublished Mathematics Table File of the American Mathematical Society. This table was constructed by Edward T. Ordman and lists $h(-p)$ for all primes p congruent to 3 modulo 4 up to 102059. A review of this and of more extensive tables is available in [11].

Tables 2, 3, 4, and 5 have been constructed by the author. Taken together, tables 2 and 3 list the dimensions of $\langle\Psi\Psi\rangle$, $\langle\Psi\Psi,E\rangle$ and V_- and the value of $\frac{(H+1)(H+2)}{2}$ for primes congruent to 3 modulo 8 between 11 and 1000. Table 4 concerns the corresponding values for primes congruent to 23 modulo 24 up to 719. Table 5 primes are those congruent to 7 modulo 24 up to 367.

The goal of this subsection is to treat the following four questions:

#1. For what values of p is E an element of $\langle\Psi\Psi\rangle$? I.e., when does $\dim\langle\Psi\Psi,E\rangle = \dim\langle\Psi\Psi\rangle$ hold?

#2. When does $\langle\Psi\Psi\rangle$ equal V_-?

#3. When are the functions in $\Psi\Psi$ linearly independent? I.e., when does $\dim\langle\Psi\Psi\rangle = \frac{(H+1)(H+2)}{2}$ hold?

#4. For what primes do we have:

$$\dim\langle\Psi\Psi\rangle < \min\left\{\frac{(H+1)(H+2)}{2}\ ,\ \dim V_-\right\}\ ?$$

Question #1 and #2 are related. If $E \notin \langle\Psi\Psi\rangle$, then $\dim\langle\Psi\Psi\rangle < \dim\langle\Psi\Psi,E\rangle \leq \dim V_-$, so $\langle\Psi\Psi\rangle \neq V_-$. The difficulty we will find is that considering p modulo 24 will not always enable

us to give a precise response to #1 - #4. The following remarks will indicate that the situation is rather complicated, so that more restrictive conditions must be placed on p to fully describe #1 - #4.

(i) In article (i) all primes are taken to be congruent to 11 modulo 24. #1 is partially answered by

Proposition: If $p \equiv 11 \pmod{24}$ and $\left(\frac{7}{p}\right) = -1$, then $E \notin \langle \Psi\Psi \rangle$.

Proof: The reduced forms f_j, $0 \le j \le H$, with $D(f_j) = -p$ are $[a_j, b_j, c_j]$ where $a_j \le a_{j+1}$. If $E(\tau) \in \langle \Psi\Psi \rangle$, then there exist constants A_{jk} such that

$$(*) \quad \frac{p-1}{24} + \sum_{n=1}^{\infty} \left\{ \sum_{\substack{d>0 \\ d \mid n \\ (d,p)=1}} d \right\} x^n = \sum_{0 \le j \le k \le H} A_{jk} \psi_{f_j} \psi_{f_k}(\tau) = \sum_{n=0}^{\infty} C_n x^n .$$

Since $\left(\frac{2}{p}\right) = -1$, we obtain $C_1 = 4A_{00} + 2 \sum_{k=1}^{H} A_{0k}$, $C_2 = 4A_{00}$, and $C_4 = 4A_{00} + 4A_{01} + 2 \sum_{k=1}^{H} A_{0k}$. Comparing with the left-hand side of (*), we obtain $A_{00} = \frac{3}{4}$ and $A_{01} = \frac{3}{2}$.

If $\left(\frac{5}{p}\right) = -1$, then $15 = C_8 = 4A_{00}$, so that $A_{00} = \frac{15}{4}$, a contradiction. If $\left(\frac{5}{p}\right) = 1$, then $8 = C_7 = 4A_{01}$, so that $A_{01} = 2$, a contradiction. Hence, $E \notin \langle \Psi\Psi \rangle$.

The proposition implies also that $\langle \Psi\Psi \rangle \neq V_-$ for $\left(\frac{7}{p}\right) = -1$, so #1 and #2 are partially answered.

When $p \equiv 11 \pmod{24}$, we know from (23) that $\dim V_- = \frac{p+13}{24} + 2H + 1$. An examination of the Ordman table yields: $\frac{(H+1)(H+2)}{2} > \dim V_-$ for the primes listed on Table 1. Hence, for at least these primes, the functions in $\Psi\Psi$ are not linearly independent. On the other hand, for the primes on Table 2, these functions are linearly independent. So both cases are possible in #3.

Regarding #4, the primes on Table 2 satisfy

$$\dim\langle\Psi\Psi\rangle = \min\left\{\frac{(H+1)(H+2)}{2},\ \dim V_-\right\} .$$

To find a counter-example, we need only determine a prime p such that $\left(\frac{7}{p}\right) = -1$ and $\dim V_- \le \frac{(H+1)(H+2)}{2}$. This is equivalent to $\left(\frac{7}{p}\right) = -1$ and $h(-p) \ge 2 + \sqrt{\frac{p+16}{3}}$. Such a p does not appear on the Ordman table. However, assuming the existence of such a prime, we obtain the desired counter-example.

(ii) We next treat #1 - #4 for the case $p \equiv 19 \pmod{24}$.

Regarding #1, we have $E \notin \langle\Psi\Psi\rangle$. To see this, we proceed as in (i) and obtain from (*) the contradiction $C_3 = 0$, since now both $\left(\frac{2}{p}\right)$ and $\left(\frac{3}{p}\right)$ equal -1. This implies of course, that $\langle\Psi\Psi\rangle$ does not equal V_-. So #1 and #2 are answered.

Table 3 shows that $\dim\langle\Psi\Psi\rangle = \frac{(H+1)(H+2)}{2}$ for primes (congruent to 19 modulo 24) up to 907. On the other hand, if there is a prime such that $\dim V_- \le \frac{(H+1)(H+2)}{2}$, then $\dim\langle\Psi\Psi\rangle < \min\left\{\frac{(H+1)(H+2)}{2},\ \dim V_-\right\}$ and no precise statement can be made regarding #3 or #4. When $p \equiv 19 \pmod{24}$, $\dim V_- = \frac{p+5}{24} + 2H + 1$ by (23); so that $\dim V_- \le \frac{(H+1)(H+2)}{2}$ is equivalent to $h(h-4) \ge \frac{p-4}{3}$ where $h = h(-p) = 2H + 1$. By the Ordman tables it can be seen that there is no prime (congruent to 19 modulo 24) up to 102043 for which this is true. However, a very large prime (with 30 digits, say) could be determined for which the inequality is valid. This fact was communicated to the author in a private communication with Daniel Shanks. Such a p would require $\left(\frac{q}{p}\right) = -1$ for all primes q going far beyond 157.

(iii) We now consider the case when $p \equiv 23 \pmod{24}$.

The Ordman table reveals that $\dim V_- < \frac{(H+1)(H+2)}{2}$ for $23 < p < 2927$. ($\dim V_- = \frac{p+1}{24} + H + 1$). Since $h(-23) = 3$ and $h(-2927) = 31$, we have

$$\dim V_- \geq \frac{(H+1)(H+2)}{2} \tag{25}$$

for $p = 23$ and $p = 2927$.

Regarding #1, Table 4 shows that $E \in \langle \Psi \rangle$ for $p \leq 719$. On the other hand, we will show below that for $p = 2927$, $E \notin \langle \Psi \rangle$. Hence, no complete statement can be made for #1 when $p \equiv 23 \pmod{24}$.

We now prove that $E \notin \langle \Psi \rangle$ for $p = 2927$.

The reduced forms $[a,b,c]$ with $b > 0$ of discriminant -2927 are:

$f_0 = [1,1,732]$ $\qquad$ $f_8 = [12,1,61]$

$f_1 = [2,1,366]$ $\qquad$ $f_9 = [12,7,62]$

$f_2 = [3,1,244]$ $\qquad$ $f_{10} = [16,9,47]$

$f_3 = [4,1,183]$ $\qquad$ $f_{11} = [18,5,41]$

$f_4 = [6,1,122]$ $\qquad$ $f_{12} = [18,13,43]$

$f_5 = [6,5,123]$ $\qquad$ $f_{13} = [24,7,31]$

$f_6 = [8,7,93]$ $\qquad$ $f_{14} = [24,23,36]$

$f_7 = [9,5,82]$ $\qquad$ $f_{15} = [27,23,32]$

We see that for $p = 2927$, $\left(\frac{q}{p}\right) = -1$ when $q = 5,7,11,13,17,19,$ or 23. By the following proposition, this implies that $E \notin \langle \Psi \rangle$.

Proposition: If $p \equiv 3 \pmod 4$, $p > 23$, and if $\left(\frac{q}{p}\right) = -1$ for $q = 5,7,11,17,19,$ and 23, then $E \notin \langle \Psi \rangle$.

Note that we place no conditions on p modulo 24, and we do not require 13 to be a quadratic non-residue modulo p.

Proof: For the reduced forms f_j, f_k, the coefficient of the 23^{rd} term of $\psi_{f_j}\psi_{f_k}$ is $\sum_{\ell=0}^{23} \rho(23-\ell, f_j)\rho(\ell, f_k)$. However, by the conditions on p, if n_1 and n_2 are non-negative integers whose sum is 23, then at least one of them is represented by no form. For example, $15 + 8 = 23$. But by the theory of representations of numbers by quadratic forms outlined in Section 1(b), $\rho(n,p) = 0$ if n_- is not a square. For $n = 15$, n_- is 5 or 15. Thus $\rho(15,p) = 0$ so that $\rho(15,f_j)\rho(8,f_k) = 0$ no matter which reduced forms f_j, f_k are chosen. This argument holds for each pair n_1, n_2 with $n_1+n_2 = 23$. But

$$E(\tau) = \frac{p-1}{24} + \sum_{n=1}^{\infty} \left(\sum_{\substack{d>0 \\ d|n \\ (d,p)=1}} d \right) e^{2\pi i n\tau}$$

has 24 for the coefficient of its 23^{rd} term. Thus, no linear combination of the $\psi_{f_j}\psi_{f_k}$ functions can equal $E(\tau)$, and the proposition is proved.

The proposition implies that there are infinitely many primes p with $p \equiv 23 \pmod{24}$ and $E \notin \langle\Psi\Psi\rangle$. For each of these primes, therefore, $\langle\Psi\Psi\rangle \neq V_-$. By Table 4 we know this is not true for all primes that are congruent to 23 modulo 24. Thus #2 admits no general solution.

The discussion at the beginning of (iii) implies that $\dim\langle\Psi\Psi\rangle < \frac{(H+1)(H+2)}{2}$ for primes p such that $23 < p < 2927$. On the other hand, for $p = 23$ we have $\dim\langle\Psi\Psi\rangle = \frac{(H+1)(H+2)}{2}$. Thus, regarding #3, it is not determined whether there exists a non-trivial prime for which the functions in $\Psi\Psi$ are linearly independent.

For #4, we assume the existence of a prime such that $\left(\frac{q}{p}\right) = -1$ where $q = 5,7,11,13,17,19,$ or 23 and $\dim V_- \leq \frac{(H+1)(H+2)}{2}$. Then $E \notin \langle\Psi\Psi\rangle$ so that $\dim V_- < \min\left\{\frac{(H+1)(H+2)}{2}, \dim V_-\right\}$.

(iv) The situation for primes p, $p \equiv 7 \pmod{24}$ leads again to indefinite responses to #1-#4. Table 5 shows that both $E \notin \langle\Psi\Psi\rangle$ and $E \in \langle\Psi\Psi\rangle$ are possible. For $p \equiv 7 \pmod{24}$, the previous proposition can be strengthened.

Proposition: If $p \equiv 7 \pmod{24}$, $p > 7$, and $\left(\frac{5}{p}\right) = \left(\frac{7}{p}\right) = -1$, then $E \notin \langle\Psi\Psi\rangle$.

Proof: We have $\left(\frac{2}{p}\right) = 1$ and $\left(\frac{3}{p}\right) = -1$, since $p \equiv 7 \pmod{24}$.

For $n_1, n_2 \in \mathbb{N}$ with $n_1 + n_2 = 7$, at least one of n_1 and n_2 is not represented by any form with discriminant $-p$. This follows from an argument similar to that in the previous proposition. Hence, $E \notin \langle \Psi\Psi \rangle$.

Primes are readily available from Table 5 to demonstrate both possibilities in #2 and #3. For #4, if p is such that $\left(\frac{5}{p}\right) = \left(\frac{7}{p}\right) = -1$ and $\dim V_- < \frac{(H+1)(H+2)}{2}$, then $E \notin \langle \Psi\Psi \rangle$ so that $\dim\langle \Psi\Psi \rangle < \min\left\{\frac{(H+1)(H+2)}{2}, \dim V_-\right\}$. However, there is no such prime congruent to 7 modulo 24 that appears on the Ordman table, though one suspects that such a prime would appear on a more extended table.

In summary, then, when $p \equiv 7 \pmod 8$, i.e., $p \equiv 7$ or $23 \pmod{24}$, we can state that there are infinitely many primes for which $E \notin \langle \Psi\Psi \rangle$ and there exist at least finitely many primes with $E \in \langle \Psi\Psi \rangle$. Questions regarding the linear independence of the functions in $\Psi\Psi$ or whether they span V_- cannot be answered in general terms merely by considering the congruence class of p modulo 24.

(b) Weierstrass points of $\mathcal{H}^*/\Gamma_0^*(p)$ when $p \equiv 23 \pmod{24}$.

We recall our previous notation from Section 3. $\Gamma_0^*(p) = \Gamma_0'(p) \cup \Gamma_0'(p)R$ where $R = \begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & 0 \end{pmatrix}$ and $\mathcal{S}^*$ is the Riemann surface $\mathcal{H}^*/\Gamma_0^*(p)$. $\mathcal{S}^*$ has exactly one cusp (at $i\infty$, say) and genus g^*, where $g^* = \frac{p+1}{24} - H$ by (22). For each $\psi \in \Psi$, $\psi|_{1,R}(\tau) = -i\psi(\tau)$.

If we let $F(\tau) = \frac{\varphi_1(\tau)}{\varphi_2(\tau)}$, where $\varphi_1, \varphi_2 \in \langle \Psi \rangle$ and non-zero, then clearly F is meromorphic on $\mathcal{S}^*$. Moreover, if φ_2 has no zeros in $\mathcal{H}$, then F is analytic everywhere on $\mathcal{S}^*$ except possibly

at $i\infty$. This suggests a consideration of the Weierstrass points of the surface.

Let $\mathfrak{R}$ be a compact Riemann surface of genus $g \geq 2$. Let P be a point of $\mathfrak{R}$. If $N \geq 2g$, $N \in \mathbb{N}$, then there exists a meromorphic function on $\mathfrak{R}$ with N poles at P and no other poles on $\mathfrak{R}$. $n \in \{1,2,\ldots,2g\}$ is called a gap if there exists no meromorphic function on $\mathfrak{R}$ with exactly n poles at P and no other poles on $\mathfrak{R}$. In the set $\{1,2,\ldots,2g\}$, exactly g numbers are gaps. P is an ordinary point if the set of gaps is $\{1,2,\ldots,g\}$. Otherwise, P is a Weierstrass point; i.e., some $n \leq g$ is a non-gap.

We wish to find, therefore, a function $\varphi \in \langle\Psi\rangle$ that is non-zero in $\mathfrak{H}$. From Section 2, we know that φ^2 is an entire modular form of dimension -2 for $\Gamma_0'(p)$, so that φ^2 has $\frac{p+1}{6}$ zeros (w.r.t. the local coordinate) in $\mathfrak{H}^*/\Gamma_0(p)$. But if φ is never zero in $\mathfrak{H}$, these zeros must be at the two cusps 0 and $i\infty$ of $\mathfrak{H}^*/\Gamma_0(p)$. That is, we must have:

$$\varphi^2(\tau) = a_0 x^{\frac{p+1}{12}} + \ldots , \quad x = e^{2\pi i\tau} , \text{ and } a_0 \neq 0, \text{ at } i\infty$$

$$\tau^2\varphi^2(\tau) = -\frac{1}{p} a_0 x^{\frac{p+1}{12}} + \ldots, \quad x = e^{\frac{2\pi i}{p}S(\tau)} \text{ at } 0 .$$

The function φ must then have the expansion

$$\varphi(\tau) = b_0 x^{\frac{p+1}{24}} + \ldots , \quad x = e^{2\pi i\tau} , \quad b_0 \neq 0 .$$

Of course, $\frac{p+1}{24}$ must be an integer since $\varphi \in \langle\Psi\rangle$, so that we must have $p \equiv 23 \pmod{24}$. In this case, $f_1 = [6,1,\frac{p+1}{24}]$ and $f_2 = [6,5,\frac{p+1}{24}+1]$ are reduced forms of discriminant $-p$ as long as we also have $p > 108$. This is due to the fact that $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1$ so that 6 is represented a total of 8 times. By Proposition 2 in Section 1(b),

we can write:

$$\psi_{f_1}(\tau) = 1 + 2 \sum_{6t^2 < \frac{p+1}{24}} x^{6t^2} + 2x^{\frac{p+1}{24}} + \dots , \quad x = e^{2\pi i \tau}$$

$$\psi_{f_2}(\tau) = 1 + 2 \sum_{6t^2 < \frac{p+1}{24}} x^{6t^2} + 2x^{\frac{p+1}{24}+1} + \dots .$$

Note that $\rho\left(\frac{p+1}{24}, f_2\right) = 0$, since otherwise $\frac{p+1}{24}$ would have to be of the form $6t^2$, which is impossible since p is prime. Hence,

$$\psi_{f_1} - \psi_{f_2} = 2x^{\frac{p+1}{24}} + \dots .$$

In particular, $\frac{p+1}{24} \in \mathrm{ORD}\langle\psi\rangle$. We let

$$F(\tau) = \frac{\varphi(\tau)}{\psi_{f_1}(\tau) - \psi_{f_2}(\tau)}$$

where $\varphi \in \langle\psi\rangle$, so that F is analytic everywhere on $\mathfrak{S}^*$ except possibly at $i\infty$. As we saw in Section 3, since $\mathrm{ord}_{i\infty}\varphi \in \mathrm{ORD}\langle\psi\rangle$, $0 \le \mathrm{ord}_{i\infty}\varphi \le \frac{p+1}{24}$ unless φ is identically zero. Thus, at $i\infty$ the number of poles of F is

$$\frac{p+1}{24} - \mathrm{ord}_{i\infty}\varphi ,$$

which is a non-negative integer not greater than $\frac{p+1}{24}$. This discussion leads to the following result.

Proposition: $i\infty$ is a Weierstrass point of $\Gamma_0^*(p)$, $p \equiv 23 \pmod{24}$, except for $p \in \{23, 47, 71, 167, 191, 239, 311\}$, in which cases $i\infty$ is ordinary.

Proof: If $0 < \frac{p+1}{24} - v \le g^* = \frac{p+1}{24} - H$ for some $v \in \mathrm{ORD}\langle\psi\rangle$, then $\frac{p+1}{24} - v$ is a non-gap, which implies that some gap is larger than g^*, so that $i\infty$ is a Weierstrass point. Hence, we must show:

$H \le v < \frac{p+1}{24}$ for some $v \notin ORD\langle\Psi\rangle$. We let $ORD\langle\Psi\rangle = \{v_0, v_1, \ldots, v_H\}$ where $0 = v_0 < v_1 < \ldots < v_H = \frac{p+1}{24}$. Therefore, if $v_{H-1} \ge H$, $i\infty$ is a Weierstrass point. We claim:

(i) $p > 71$ implies $g^* = \frac{p+1}{24} - H \ge 2$, and

(ii) $v_{H-1} > H-1$ except for $p \in \{23,47,71,167,191,239,311\}$. A few simple calculations (cf. Table 4) show that (i) and (ii) hold up to $p = 983$. Thus, assume $p > 983$.

It is known ([6], pg. 196) that $h(-p) = \frac{\sqrt{p}}{\pi} K(-p)$, where $K(-p) = \sum_{n=1}^{\infty} \frac{1}{n}\left(\frac{-p}{n}\right)$. Using the fact (cited in [7], pg. 367) that $K(-p) \le 2\log 4p$, we have $h(-p) \le \frac{2\sqrt{p}}{\pi} \log 4p$. But $p > 40691$ implies $\frac{2\sqrt{p}}{\pi} \log 4p \le \frac{p+1}{24} + 2$, so $h(-p) \le \frac{p+1}{24} + 2$. It is easy to check from the Ordman table that this last inequality holds for all primes up to and including 40691 that are congruent to 23 modulo 24. Therefore, we have $H-1 < \frac{p+1}{48}$.

Since $p > 983$ and $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1$, the theory of representations by quadratic forms implies that $\rho(12,p) = 12$. Hence, either $\left[12,1,\frac{p+1}{48}\right]$ and $\left[12,7,\frac{p+1}{48}+1\right]$ or $\left[12,5,\frac{p+25}{48}\right]$ and $\left[12,11,\frac{p+25}{48}+2\right]$ are reduced. Thus, either $\frac{p+1}{48}$ or $\frac{p+25}{48}$ is an element of $ORD\langle\Psi\rangle$. We have, then, $H-1 < \frac{p+1}{48} \le v_{H-1}$ and (ii) follows.

For (i), $p > 983$ implies $3 \le H$. This together with $H-1 < \frac{p+1}{48}$ yields $2 \le H-1 \le \frac{p+1}{24} - H = g^*$.

(c) Zeros of $\psi(\tau)$ in $\mathcal{H}$

In the previous subsection we exhibited a function $\varphi \in \langle\Psi\rangle$ which is never zero in $\mathcal{H}$. There the space $\langle\Psi\rangle$ corresponded to a prime p with $p \equiv 23 \pmod{24}$. If $p \equiv 3 \pmod 8$, on the other hand, we

will show that no such function φ exists in the space $\langle\Psi\rangle$. In fact, we will write down explicitly a set of $h(-p)$ points in $\mathfrak{H}$ that are non-equivalent under $\Gamma_0(p)$ and at which each function $\psi \in \Psi$ is zero. The basic argument underlying the proof is due to Fricke.

We recall that for $p \equiv 3 \pmod 4$, $p > 3$, the transformation $R: \tau \to \frac{-1}{p\tau}$ determines the analytic involution $R^*: \langle\tau\rangle \to \langle R\tau\rangle$ on $\mathfrak{H}^*/\Gamma_0(p)$. The fixed points of R^* are precisely those points $\langle\tau\rangle$ where $\tau = \frac{b}{d} + \frac{i}{d\sqrt{p}} \in \mathfrak{H}$. For, $\langle\tau\rangle = \langle R\tau\rangle$ if, and only if, $\tau = VR\tau$ for some $V = \begin{pmatrix} a & b \\ cp & d \end{pmatrix} \in \Gamma_0'(p)$. But $\Gamma_0(p)R$ has order 2 in $\Gamma_0^*(p)/\Gamma_0(p)$ so that $(VR)^2 \in \Gamma_0(p)$. Since $(VR)^2$ fixes $\tau \in \mathfrak{H}$, $(VR)^2$ is elliptic or the identity. As an element of Γ',

$$(VR)^2 = \begin{pmatrix} b^2p - ad & a(c - b) \\ dp(b - c) & c^2p - ad \end{pmatrix}.$$

If $(VR)^2$ as an element of Γ has order 2, then by the general theory of elliptic transformations we must have $(b^2p - ad) + (c^2p - ad) = 0$, which is impossible. Similarly, if $(VR)^2$ as an element of Γ has order 3, then $(b^2p - ad) + (c^2p - ad) = \epsilon$ where $\epsilon = +1$ or -1. But $ad = bcp + 1$, so p must divide $\epsilon + 2$, which is impossible. Therefore, $(VR)^2 = \epsilon I$ where again $\epsilon = +1$ or -1. It follows that $b = c$, so $V = \begin{pmatrix} a & b \\ bp & d \end{pmatrix}$.

A simple calculation now shows that τ must equal $\frac{b}{d} + \frac{i}{d\sqrt{p}}$. We thus obtain a one-to-one correspondence

$$\tau = \frac{b}{d} + \frac{i}{d\sqrt{p}} \longleftrightarrow V = \begin{pmatrix} a & b \\ bp & d \end{pmatrix} \in \Gamma_0'(p) \text{ with } d > 0.$$

Furthermore, V determines $f_v = [\epsilon a, 2\epsilon bp, \epsilon dp]$, where

$$\epsilon = \begin{cases} \frac{1}{2}, & \text{if } a \equiv d \equiv 0 \pmod 2 \\ 1, & \text{otherwise.} \end{cases}$$

Then f_v is a primitive, positive-definite form and

$$D(f_v) = \begin{cases} -p, & \text{if } a \equiv d \equiv 0 \pmod 2, \text{ and} \\ -4p, & \text{otherwise.} \end{cases}$$

This correspondence generates a 1-1 correspondence between equivalent points and properly equivalent forms as the following proposition shows.

Proposition 1: Let F be the set of points of $\mathcal{H}^*/\Gamma_0(p)$ that are fixed by R^*. Let $\mathfrak{F}$ be the set of equivalence classes of forms determined by the forms f which satisfy:

(*) $f = [A, Bp, Dp]$ is primitive, positive-definite, and

$$D(f) = \begin{cases} -p, & \text{if } B \text{ odd} \\ -4p, & \text{if } B \text{ even} \end{cases}$$

Then

(i) Every primitive, positive-definite form of discriminant $-p$ or $-4p$ is equivalent to a form satisfying (*).

(ii) If f_1 and f_2 are properly equivalent and satisfy (*), then $f_1{}^t U = f_2$ for some $U \in \Gamma_0'(p)$, where ${}^t U$ is the transpose of U.

(iii) F and $\mathfrak{F}$ are in 1-1 correspondence.

Proof: (i) If f does not satisfy (*) and $f = [A,B,C]$ is primitive and positive-definite with $D(f) = -p$, then for some

$$M = \begin{pmatrix} x_1 & -2C \\ x_3 & B \end{pmatrix} \in \Gamma',$$

$$fM = [f(x_1,x_3), -x_1 p, Cp]$$

satisfies (*). Similarly, if f does not satisfy (*) and $D(f) = -4p$,

then for some

$$M = \begin{pmatrix} x_1 & -C \\ x_3 & \frac{B}{2} \end{pmatrix} \in \Gamma' ,$$

$$fM = [f(x_1,x_3),\ -2x_1p,Cp]$$

satisfies (*).

(ii) Let $f_1 = [A_1,B_1p,C_1p]$ and $f_2 = [A_2,B_2p,C_2p]$. Say $f_1{}^tU = f_2$ where $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma'$. Then $f_1{}^tU\begin{pmatrix} 0 \\ 1 \end{pmatrix} = f_2\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ implies

$$A_1\gamma^2 + pB_1\gamma\delta + C_1p\delta^2 = C_2p .$$

But $(A_1,p) = 1$, so p divides γ and $U \in \Gamma_0'(p)$.

(iii) If $\langle\tau\rangle \in F$, then

$$\tau = \frac{b}{d} + \frac{i}{d\sqrt{p}} \quad \rightarrow \quad V = \begin{pmatrix} a & b \\ bp & d \end{pmatrix} \in \Gamma_0'(p),\ d > 0$$

is a 1-1 correspondence between fixed points in $\mathcal{H}$ and elements of $\Gamma_0'(p)$ of the form $\begin{pmatrix} a & b \\ bp & d \end{pmatrix}$, $d > 0$. As remarked above, each such V determines $f_v = [\epsilon a,\ 2\epsilon bp,\ \epsilon dp]$, which satisfies (*). If $U \in \Gamma_0'(p)$ and $\tau_1 = U\tau$, then τ_1 determines $V_1 = UVRU^{-1}R^{-1}$, which corresponds to $f_{v_1} = f_v{}^tU$. The above maps are reversible, so that $\mathfrak{F}$ and F are in 1-1 correspondence. Hence (iii) is proved.

Clearly, if τ_0 determines a point of $\mathcal{H}^*/\Gamma_0(p)$ that is fixed by R^*, then $\left[\left(\frac{d}{p}\right) - 1\right]\psi(\tau_0) = 0$ where $\tau_0 = \frac{b}{d} + \frac{i}{d\sqrt{p}}$ and $\psi \in \Psi$.

For, τ_0 is fixed by $VR = \begin{pmatrix} a & b \\ bp & d \end{pmatrix}R$, so that

$$\psi_{\big|_{1,VR}}(\tau_0) = \frac{1}{d\sqrt{p}\tau_0 - b\sqrt{p}}\ \psi(VR\tau_0) = \frac{1}{i}\psi(\tau_0) = -i\psi(\tau_0)$$

by definition of the "stroke" operation. On the other hand, by (10) and (17),

$$\psi\Big|_{1,VR}(\tau_0) = -i\left(\frac{d}{p}\right)\psi(\tau_0) .$$

Hence, $\left[\left(\frac{d}{p}\right) - 1\right]\psi(\tau_0) = 0$. To insure that $\psi(\tau_0) = 0$, we require the conditions under which $\left(\frac{d}{p}\right) = -1$.

Lemma: If $p \equiv 3 \pmod 4$, $p > 3$, $V = \begin{pmatrix} a & b \\ bp & d \end{pmatrix} \in \Gamma_0'(p)$ with $d > 0$, then $\left(\frac{d}{p}\right) = -1$ if, and only if, $d \equiv 2 \pmod 4$ and $p \equiv 3 \pmod 8$.

Proof:

Necessity: Clearly $d \neq 1$. Furthermore, d must be even, since $\left(\frac{d}{p}\right) = 1$ when d is odd. For, let $d = q_1 q_2 \cdots q_j$, where each q_j is a prime and the q_j are not necessarily distinct, each $q_j > 2$ and relatively prime to p. Then $ad - b^2p = 1$ implies $-4p \equiv (2bp)^2 \pmod d$, so $\left(\frac{-4p}{d}\right) = 1$. On the other hand,

$$\left(\frac{-4p}{d}\right) = \prod_j \left(\frac{-4}{q_j}\right) \cdot \prod_j \left(\frac{p}{q_j}\right) = \prod_j \left(\frac{-1}{q_j}\right) \cdot \prod_j \left(\frac{q_j}{p}\right)(-1)^{\frac{p-1}{2}\,\frac{q_j-1}{2}} = \left(\frac{d}{p}\right)$$

since $p \equiv 3 \pmod 4$. Thus, $\left(\frac{d}{p}\right) = 1$ if d is odd.

Therefore, we may assume that d is even. Let $d = 2^k D$, $k \geq 1$, where D is odd. Since $2^k aD - b^2 p = 1$, the above argument applied to D in place of d shows that $\left(\frac{D}{p}\right) = 1$. Then

$$-1 = \left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)^k \left(\frac{D}{p}\right) = \left(\frac{2}{p}\right)^k = (-1)^{k\,\frac{p^2-1}{8}} \text{ , so that } p \equiv 3 \pmod 8.$$

Finally, we show that 4 does not divide d. Since clearly $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = -1$, the above paragraph shows that a is also even. Consequently, if 4 were to divide d, then $1 = ad - b^2p \equiv -b^2p \equiv -3b^2 \pmod 8$ would imply that $b^2 \equiv 5 \pmod 8$, a contradiction. Hence, $d \equiv 2 \pmod 4$ and necessity is proved.

Sufficiency: Let $d = 2D$ where D is odd. Then $1 = 2aD - b^2p$ and the first paragraph of the proof imply that $1 = \left(\frac{D}{p}\right)$. Since $p \equiv 3 \pmod 8$, $\left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{D}{p}\right) = \left(\frac{2}{p}\right) = -1$, and the proof is complete.

The above lemma allows us to state:

Proposition 2: If $p \equiv 3 \pmod 8$ and $f = [A,Bp,Dp]$ is primitive and positive-definite with discriminant $-p$, then $\psi\left(\frac{B}{2D} + \frac{i}{2D\sqrt{p}}\right) = 0$.

Proof: By the correspondence between points fixed under R^* and forms, we have

$$f = [A,Bp,Dp] \rightarrow V = \begin{pmatrix} 2A & B \\ Bp & 2D \end{pmatrix} \rightarrow \tau_0 = \frac{B}{2D} + \frac{i}{2D\sqrt{p}} .$$

Thus, $\left[\left(\frac{2D}{p}\right) - 1\right] \psi(\tau_0) = 0$. Furthermore, D is odd. Otherwise, $1 = 4AD - B^2p \equiv -B^2p \equiv -3B^2 \pmod 8$ implies $B^2 \equiv 5 \pmod 8$, which is impossible. Hence, by the lemma, $\left(\frac{2D}{p}\right) = -1$, so $\psi(\tau_0) = 0$.

But we have seen that every positive-definite form of discriminant $-p$ is properly equivalent to a form f such as in the previous proposition, and non-equivalent forms correspond to non-equivalent points. We summarize our results:

Theorem: If $p \equiv 3 \pmod 8$, $p > 3$, then each $\psi \in \Psi$ has at least $h(-p)$ non-equivalent points τ_0 for which $\psi(\tau_0) = 0$. These are determined by precisely those points $\tau_0 = \frac{B}{2D} + \frac{i}{2D\sqrt{p}} \in \mathcal{H}$ where $[A,Bp, Dp]$ is a positive-definite form with discriminant $-p$.

SECTION 5: TABLES

TABLE 1

$p \equiv 11 \pmod{24}$, $11 \leq p \leq 102,059$; $\frac{(H+1)(H+2)}{2} > \dim V_{-} = \frac{p+13}{24} + 2H+1$

p	H	h	$\frac{(H+1)(H+2)}{2}$	$\dim V_{-}$
28019	49	99	1275	1267
48179	64	129	2145	2137
58211	71	143	2628	2569
58379	71	143	2628	2576
63131	74	149	2850	2780
59219	76	153	3003	2621
70979	79	159	3240	3117
66491	82	165	3486	2936
78179	83	167	3570	3425
77171	84	169	3655	3385
84059	85	171	3741	3674
74051	87	175	3916	3261
85931	87	175	3916	3756
95651	90	181	4186	4167
97499	92	185	4371	4248
94331	93	187	4465	4118
96851	95	191	4656	4227
100019	96	193	4753	4361

TABLE 2

$p \equiv 11 \pmod{24}$; $11 \leq p \leq 971$

p	H	h	dim$\langle\Psi\Psi\rangle$	dim$\langle\Psi\Psi, E\rangle$	$\frac{(H+1)(H+2)}{2}$	dim V_-
11	0	1	1	2	1	2
59	1	3	3	4	3	6
83	1	3	3	4	3	7
107	1	3	3	4	3	8
131	2	5	6	7	6	11
179	2	5	6	7	6	13
227	2	5	6	7	6	15
251	3	7	10	11	10	18
347	2	5	6	7	6	20
419	4	9	15	16	15	27
443	2	5	6	7	6	24
467	3	7	10	11	10	27
491	4	9	15	16	15	30
563	4	9	15	16	15	33
587	3	7	10	11	10	32
659	5	11	21	22	21	39
683	2	5	6	7	6	34
827	3	7	10	11	10	42
947	2	5	6	7	6	45
971	7	15	36		36	56

TABLE 3

$p \equiv 19 \pmod{24}$; $19 \leq p \leq 907$

p	H	h	$\dim\langle\Psi\Psi\rangle$	$\dim\langle\Psi\Psi,E\rangle$	$\frac{(H+1)(H+2)}{2}$	$\dim V_-$
19	0	1	1	2	1	2
43	0	1	1	2	1	3
67	0	1	1	2	1	4
139	1	3	3	4	3	9
163	0	1	1	2	1	8
211	1	3	3	4	3	12
283	1	3	3	4	3	15
307	1	3	3	4	3	16
331	1	3	3	4	3	17
379	1	3	3	4	3	19
499	1	3	3	4	3	24
523	2	5	6	7	6	27
547	1	3	3	4	3	26
571	2	5	6	7	6	29
619	2	5	6	7	6	31
643	1	3	3	4	3	30
691	2	5	6	7	6	34
739	2	5	6	7	6	36
787	2	5	6	7	6	38
811	3	7	10	11	10	41
859	3	7	10	11	10	43
883	1	3	3	4	3	40
907	1	3	3	4	3	41

$p \equiv 23 \pmod{24}$; $23 \leq p \leq 719$

p	H	h	dim$\langle\Psi\Psi\rangle$	dim$\langle\Psi\Psi, E\rangle$	$\frac{(H+1)(H+2)}{2}$	dim V_-	g^*	gaps
* 23	1	3	3	3	3	3	0	-------
* 47	2	5	5	5	6	5	0	-------
* 71	3	7	7	7	10	7	0	-------
*167	5	11	13	13	21	13	2	1,2
*191	6	13	15	15	28	15	2	1,2
*239	7	15	18	18	36	18	3	1,2,3
263	6	13	18	18	28	18	5	1,2,3,4,6
*311	9	19	23	23	55	23	4	1,2,3,4
359	9	19	25	25	55	25	6	1,2,3,4,5,8
383	8	17	25	25	45	25	8	1,2,...,7,11
431	10	21	29	29	66	29	8	1,2,...,6,8,11
479	12	25	33	33	91	33	8	1,2,...,7,9
503	10	21	32	32	66	32	11	1,2,...,9,11,16
599	12	25	38	38	91	38	13	1,2,...,9,11,13,14,18
647	11	23	39	39	78	39	16	1,...,12,14,16,17,22
719	15	31	46	46	136	46	15	1,...,11,13,14,16,19

TABLE 4

Note: * $i\infty$ not a Weierstrass point

TABLE 5

$p \equiv 7 \pmod{24}$; $7 \leq p \leq 367$

p	H	h	$\dim\langle\Psi\Psi\rangle$	$\dim\langle\Psi\Psi, E\rangle$	$\frac{(H+1)(H+2)}{2}$	$\dim V_-$
7	0	1	1	1	1	1
31	1	3	3	3	3	3
79	2	5	6	6	6	6
103	2	5	6	7	6	7
127	2	5	6	7	6	8
151	3	7	10	10	10	10
199	4	9	13	13	15	13
223	3	7	10	11	10	13
271	5	11	17	17	21	17
367	4	9	15	16	15	20

BIBLIOGRAPHY

[1] Borevich, Z.I. and Shafarevich, I.R., Number Theory, Academic Press, New York, 1966.

[2] Cohn, Harvey, A Second Course in Number Theory, John Wiley and Sons, New York, 1962.

[3] Dickson, Eugene D., Introduction to the Theory of Numbers, Dover Publications, New York, 1957.

[4] Hecke, Erich, "Zur Theorie der elliptischen Modulfunktionen," Mathematischen Annalen, Bd. 97, (1926), pp. 210-42. = Math. Werke, pp. 428-60.

[5] Hecke, Erich, "Theorie der Eisensteinischen Reihen hoherer Stufe und ihre Anwendung auf Funktionentheorie und Arithmetik," Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universitat, Bd. 5, (1927), pp. 199-224. = Math. Werke, pp. 461-86.

[6] Landau, Edmund, Elementary Number Theory, Chelsea Publishing Co., New York, 1966.

[7] Lehner, J. and Newman, M., "Weierstrass Points of $\Gamma_0(N)$," Annals of Mathematics, 79(1964), pp. 360-68.

[8] Lewittes, J., "Construction of Modular Forms," to appear.

[9] Ordman, Edward T., "Tables of the Class Number for Negative Prime Discriminants," Unpublished Mathematics Table File of the American Mathematics Society, Providence, Rhode Island.

[10] Schoeneberg, B., Elliptic Modular Functions, Springer-Verlag, New York, 1974.

[11] Shanks, Daniel, Mathematics of Computation, 23(1969), p. 458.

_____, Mathematics of Computation, 24(1970), p. 491-3.

[12] Springer, George, Introduction to Riemann Surfaces, Addison-Wesley Publishing Co., Reading, Mass., 1957.