DIRICHLET SERIES

BY

A. C. Schaeffer†

Editor's Remark. This paper was written by the author shortly before his untimely death in 1957, in order to crystallize his thinking on a subject which was occupying a large part of his attention at the time. While the paper is largely expository and while the principal object of the author was not achieved, the material discussed is significant and seems worth presenting to the mathematical public in order to stimulate further research.

In the paper after this one, Mr. Hwa Suk Hahn has verified Schaeffer's conjectures for $p = 3, 5,$ and 7, and indicated some of the difficulties that arise for larger values of p. Schaeffer had apparently carried out these verifications also, at least for $p = 3$ and 5.

The editors would like to thank the following mathematicians who have assisted in one way or another in the publication of this paper: R. C. Buck, Albert Edrei, Hwa S. Hahn, Norman Hamilton, Marvin I. Knopp, Morris Newman, and Hans Rademacher.

Paul T. Bateman

I. Introduction

Let

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

be the L-function corresponding to a Dirichlet character function $\chi(n)$ modulo k. In case $k > 1$ and $\chi(-1) = 1$ the L-function is the transform of

$$\psi(\tau, \chi) = \sum_{-\infty}^{\infty} \chi(n) e^{i\pi n^2 \tau/k}$$

in the sense that, for Re $s > 1$,

$$2\Gamma\left(\frac{s}{2}\right)\left(\frac{k}{\pi}\right)^{s/2} L(s, \chi) = \int_0^{\infty} u^{s/2-1} \psi(iu, \chi)\, du.$$

In view of the importance of the L-functions in analytic number theory it is of interest to give a function-theoretic definition of their transforms $\psi(\tau, \chi)$, that is, a definition of ψ which will depend on its characteristic properties rather than on any special representation. Earlier work of Hamburger [2, 3, 4], Siegel [11], and Hecke [5, 6] can be interpreted as contributions in this direction. The results of Hamburger and Siegel, which are stated in terms of the L-functions rather than their transforms ψ, are in part function-theoretic. It was Hecke who systematically investigated this and related questions about modular functions. For some integers k, all of which are divisors of 24, Hecke [6] has shown that $\psi(\tau, \chi)$ is determined up to a multiplicative constant by certain functional equations which it satisfies. It is not clear how the methods

Received December 15, 1959.

of these authors can be extended to answer the questions which are to be investigated.

The present note is an attempt to define the functions $\psi(\tau, \chi)$ by means of certain functional equations which they satisfy, (8) below. Although much of the analysis can be extended to the case in which k is any positive integer, we shall, for the sake of simplicity, consider the case $k = p$ where p is an odd prime. Also $\chi(-1) = 1$. Thus

$$\psi(\tau, \chi) = \sum_{-\infty}^{\infty} \chi(n) e^{i\pi n^2 \tau / p}, \qquad \chi(-1) = 1. \tag{1}$$

It is clear that $\psi(\tau, \chi)$ is regular in $\operatorname{Im}(\tau) > 0$, and it satisfies

$$| \psi(x + iy, \chi) | \leqq A(1 + y^{-c}), \qquad y > 0, \tag{2}$$

where A, c are some positive numbers. (It can in fact be shown that we may take $c = \frac{1}{2}$.)

Let $H(1)$ be the group of transformations $(\alpha\tau + \beta)/(\gamma\tau + \delta)$ where α, β, γ, δ are integers with

$$\alpha\delta - \beta\gamma = 1, \qquad \alpha + \delta \equiv \beta + \gamma \equiv 0 \pmod 2.$$

Consider the following subgroups of $H(1)$:

$$\begin{array}{lcr} R(p), & \beta \equiv 0 & (\text{mod } p), \\ H(p), & \gamma \equiv \beta \equiv 0 & (\text{mod } p), \\ \Gamma(p), & \gamma \equiv \beta \equiv 0, \quad \alpha \equiv \delta \equiv \pm 1 & (\text{mod } p). \end{array}$$

It is clear that $\Gamma(p)$ is an invariant subgroup of $H(1)$. Write $D_H(1)$, $D_R(p)$, $D_H(p)$, $D_\Gamma(p)$ for fundamental domains of the corresponding groups. Thus $D_H(1)$ may be taken as the set

$$\operatorname{Im}(\tau) \geqq 0, \qquad -1 \leqq \operatorname{Re}(\tau) \leqq 1, \qquad | \tau | \geqq 1,$$

where boundary arcs are identified in pairs by the transformations $-1/\tau$, $\tau + 2$ which generate $H(1)$.

The function

$$\vartheta(\tau) = \sum_{-\infty}^{\infty} e^{i\pi n^2 \tau} \tag{3}$$

satisfies the functional equations

$$\vartheta(\tau + 2) = \vartheta(\tau), \qquad \vartheta(-1/\tau) = (-i\tau)^{1/2} \vartheta(\tau).$$

Here and elsewhere the square root has nonnegative real part. It is also known that if $(\alpha\tau + \beta)/(\gamma\tau + \delta)$ is any transformation belonging to $H(1)$ then

$$\vartheta\left(\frac{\alpha\tau + \beta}{\gamma\tau + \delta}\right) = S(\gamma\tau + \delta)^{1/2} \vartheta(\tau), \tag{4}$$

where

$$(5) \qquad S = \begin{cases} \left(\dfrac{\gamma}{\delta}\right) e^{(i\pi/4)(\delta-1)} & \text{if } \beta, \gamma \text{ are even}, \quad \delta > 0, \\ \left(\dfrac{\delta}{\gamma}\right) e^{-(i\pi/4)\gamma} & \text{if } \alpha, \delta \text{ are even}, \quad \gamma > 0. \end{cases}$$

Here $\left(\dfrac{a}{b}\right)$ is the Jacobi symbol, and $\left(\dfrac{a}{1}\right) = 1$. Defining

$$\phi(\tau) = \vartheta(\tau/p)$$

it follows from (4) that if $(\alpha\tau + \beta)/(\gamma\tau + \delta) \in R(p)$ then

$$(6) \qquad \phi\left(\frac{\alpha\tau + \beta}{\gamma\tau + \delta}\right) = S'(\gamma\tau + \delta)^{1/2}\phi(\tau),$$

where

$$(7) \qquad S' = \begin{cases} \left(\dfrac{p\gamma}{\delta}\right) e^{(i\pi/4)(\delta-1)} & \text{if } \beta, \gamma \text{ are even}, \quad \delta > 0, \\ \left(\dfrac{\delta}{p\gamma}\right) e^{-(i\pi/4)p\gamma} & \text{if } \alpha, \delta \text{ are even}, \quad \gamma > 0. \end{cases}$$

It will be shown that if $(\alpha\tau + \beta)/(\gamma\tau + \delta) \in H(p)$ then

$$(8) \qquad \psi\left(\frac{\alpha\tau + \beta}{\gamma\tau + \delta}, \chi\right) = S'\chi(\delta)(\gamma\tau + \delta)^{1/2}\psi(\tau, \chi).$$

A question which now arises is whether the functional equations (8) and the order relation (2) determine $\psi(\tau, \chi)$ up to a multiplicative constant. In the case of the principal character function χ_0 some qualification must be made. For

$$\psi(\tau, \chi_0) = \vartheta(\tau/p) - \vartheta(p\tau),$$

and both the functions $\vartheta(\tau/p)$ and $\vartheta(p\tau)$ transform according to (6) in $H(p)$. It is more convenient to state the question for transformations in $\Gamma(p)$. In case $(\alpha\tau + \beta)/(\gamma\tau + \delta)$ belongs to $\Gamma(p)$ we have $\chi(\delta) = 1$, so the $(p + 1)/2$ functions $\phi(\tau)$ and $\psi(\tau, \chi)$ transform according to the same rule in $\Gamma(p)$. The question to be investigated in the present note is the following: *If $\psi(\tau)$ is regular in* $\operatorname{Im}(\tau) > 0$ *where it satisfies*

$$(9) \qquad \psi\left(\frac{\alpha\tau + \beta}{\gamma\tau + \delta}\right) = S'(\gamma\tau + \delta)^{1/2}\psi(\tau)$$

in $\Gamma(p)$ and the order relation

$$(10) \qquad |\psi(x + iy)| \leqq A(1 + y^{-c}),$$

must $\psi(\tau)$ be a linear combination of the $(p + 1)/2$ functions $\phi(\tau)$, $\psi(\tau, \chi)$?

Relations (6), (8) show that the $(p + 1)/2$ functions

$$1, \qquad \psi(\tau, \chi)/\phi(\tau)$$

are automorphic under the group $\Gamma(p)$, and they are regular in the fundamental domain $D_\Gamma(p)$ of $\Gamma(p)$ except for poles at the places where $\phi(\tau)$ has a zero of higher order than does $\psi(\tau, \chi)$. It will be shown that there is a divisor Q' on $D_\Gamma(p)$ which consists of poles of total multiplicity

$$(p^2 - 1)(p - 1)/16$$

such that if ψ is any function which satisfies (9), (10) then $\psi(\tau)/\phi(\tau)$ is a multiple of Q'. If it can be shown that the $(p + 1)/2$ functions $1, \psi(\tau, \chi)/\phi(\tau)$ are a complete set of linearly independent multiples of Q' then it will follow that any function $\psi(\tau)$ which is regular in $\mathrm{Im}(\tau) > 0$ and satisfies (9), (10) is a linear combination of the $(p + 1)/2$ functions $\phi(\tau), \psi(\tau, \chi)$.

Now the genus of $D_\Gamma(p)$ will be shown to be

$$g = \tfrac{1}{8}(p^3 - 4p^2 - p + 12) = \tfrac{1}{8}(p - 3)(p^2 - p - 4).$$

In order to find all multiples of Q' there is defined on $D_\Gamma(p)$ another divisor Q consisting of poles of total multiplicity

$$| Q | = \tfrac{1}{4}(p^2 - 1)(p - 2),$$

which includes all poles of Q'. It is a consequence of the Riemann-Roch theorem that if $| Q | > 2g - 2$ then there are precisely $| Q | - g + 1$ linearly independent multiples of Q. The divisor Q to be defined does satisfy the condition $| Q | > 2g - 2$, so it has precisely

$$| Q | - g + 1 = (p^3 - p)/8$$

linearly independent multiples. In this paper there are exhibited $(p^3 - p)/8$ multiples of Q, but I do not know if they are linearly independent. In case they are linearly independent, then all multiples of Q' are contained in the linear space of these $(p^3 - p)/8$ functions, and it remains to show that there are precisely $(p + 1)/2$ such linearly independent functions. The proof can readily be completed in the special cases $p = 3, 5$.

There is a connection between these questions and the problem of finding all irreducible representations of the quotient group $H(1)/\Gamma(p)$. These representations have been determined by Kloosterman and others; cf. [7, 8] where the history of the problem is discussed.

There is also a connection between these questions and the problem of finding the number of representations of an integer as the sum of three or more squares; cf. Bateman [1] where further references are given.

II. The fundamental domain

The genus, a complete set of inequivalent vertices, and local uniformizers are to be found for the fundamental domain $D_\Gamma(p)$ of $\Gamma(p)$. Some of the results of this section overlap those of Newman [9] and Hecke [5, 6]. We consider the transformations $(\alpha\tau + \beta)/(\gamma\tau + \delta)$ and $(-\alpha\tau - \beta)/(-\gamma\tau - \delta)$ equal; and if a transformation $(\alpha\tau + \beta)/(\gamma\tau + \delta)$ is in a group, we shall also speak of its matrix $\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix}$ as in that group.

There are $p + 1$ right cosets

$$\begin{pmatrix}0 & -1 \\ 1 & 0\end{pmatrix}, \quad \begin{pmatrix}1 & 2\nu \\ 0 & 1\end{pmatrix}, \qquad 0 \leqq \nu \leqq p - 1, \tag{11}$$

of $R(p)$ in $H(1)$. There are p right cosets

$$\begin{pmatrix}1 & 0 \\ 2j & 1\end{pmatrix}, \qquad 0 \leqq j \leqq p - 1, \tag{12}$$

of $H(p)$ in $R(p)$. The group $H(p)/\Gamma(p)$ is cyclic of order $(p - 1)/2$. Indeed let a be an odd primitive root modulo p, and define d by

$$ad \equiv 1 \pmod{4p^2}.$$

There are b, c such that

$$U = \begin{pmatrix}a & b \\ c & d\end{pmatrix}$$

is the matrix of a transformation in $H(p)$. Then

$$U^\nu = \begin{pmatrix}a_\nu & b_\nu \\ c_\nu & d_\nu\end{pmatrix}, \qquad 1 \leqq \nu \leqq (p - 1)/2, \tag{13}$$

are cosets of $\Gamma(p)$ in $H(p)$. For $a_\nu \equiv a^\nu \pmod{p}$; and if

$$(\alpha\tau + \beta)/(\gamma\tau + \delta) \in H(p),$$

then

$$\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix}\begin{pmatrix}d_\nu & -b_\nu \\ -c_\nu & a_\nu\end{pmatrix} = \begin{pmatrix}A_\nu & B_\nu \\ C_\nu & D_\nu\end{pmatrix},$$

where

$$D_\nu \equiv \delta a_\nu \equiv \delta a^\nu \pmod{p}.$$

There is thus a unique ν in the range $1 \leqq \nu \leqq (p - 1)/2$ such that

$$D_\nu \equiv \pm 1 \pmod{p},$$

and, since $A_\nu D_\nu \equiv 1 \pmod{p}$, the transformation belongs to $\Gamma(p)$.

Choose for the fundamental domain $D_H(1)$ of $H(1)$ the set

$$\mathrm{Im}(\tau) \geqq 0, \qquad -1 \leqq \mathrm{Re}(\tau) \leqq 1, \qquad |\tau| \geqq 1,$$

where the line segments $\mathrm{Re}(\tau) = \pm 1$, $\mathrm{Im}(\tau) \geqq 0$ are identified by the transformation $\tau + 2$, and the parts of the unit circumference in the first and second quadrants are identified by the transformation $-1/\tau$. The boundary of $D_H(1)$ lies on arcs of three circles. The domain $D_R(p)$ consists of $p + 1$

images of $D_H(1)$ by the transformations with matrices (11). Thus the boundary of $D_R(p)$ lies on arcs of $p + 3$ circles. The transformations by which these boundary points are identified have matrices

$$\begin{pmatrix} 1 & 2p \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2j \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -2k \\ 0 & 1 \end{pmatrix}$$

where $1 \leqq j, k \leqq p - 1$ and $4jk + 1 \equiv 0 \pmod p$. If $p \equiv 3 \pmod 4$, then $j \neq k$, so there are no elliptic vertices. If $p \equiv 1 \pmod 4$, then there are two solutions of the congruence $4k^2 \equiv -1 \pmod p$, so there are two elliptic vertices, each of period 2. They are fixed points of transformations with matrices

$$\begin{pmatrix} -2k & 1 + 4k^2 \\ -1 & 2k \end{pmatrix}$$

where $4k^2 + 1 \equiv 0 \pmod p$, $0 < k < p$.

The domain $D_H(p)$ is the sum of p copies of $D_R(p)$ by transformations with matrices (12). Thus the boundary of $D_H(p)$ lies on arcs of $p^2 + p + 2$ circles. If $p \equiv 3 \pmod 4$, there are no elliptic vertices, and these arcs are identified in pairs. If $p \equiv 1 \pmod 4$, then for each k that satisfies $4k^2 + 1 \equiv 0 \pmod p$ there is a unique ν in the range $0 \leqq \nu < p$ such that

$$\begin{pmatrix} 1 & 0 \\ 2\nu & 1 \end{pmatrix}\begin{pmatrix} -2k & 1 + 4k^2 \\ -1 & 2k \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -2\nu & 1 \end{pmatrix}$$

is the matrix of a transformation belonging to $H(p)$. Thus there are two elliptic vertices. If $p \equiv 1 \pmod 4$, then the domain $D_H(p)$ has $p^2 + p + 4$ boundary arcs which are identified in pairs, it has two elliptic vertices, each of period 2, and it has $p^2 + p + 2$ parabolic vertices.

The domain $D_\Gamma(p)$ is the sum of $(p - 1)/2$ images of $D_H(p)$. Let these images be contiguous. Then the boundary of $D_\Gamma(p)$ lies on arcs of

$$(p^3 - p + 4)/2$$

circles. These arcs are identified by transformations in $\Gamma(p)$. There are no elliptic vertices in $D_\Gamma(p)$. For if τ_0 is a fixed point of

$$(\alpha\tau + \beta)/(\gamma\tau + \delta) \in \Gamma(p)$$

and $\operatorname{Im}(\tau_0) > 0$, then

$$2\gamma\tau_0 = \alpha - \delta \pm \sqrt{(\alpha + \delta)^2 - 4}.$$

Since $\alpha + \delta$ is even, this implies that $\alpha + \delta = 0$. But $\alpha \equiv \delta \equiv \pm 1 \pmod p$, so $\alpha + \delta \equiv \pm 2 \pmod p$, which is impossible, since p is odd. Thus the fundamental domain $D_\Gamma(p)$ of $\Gamma(p)$ is bounded by $(p^3 - p + 4)/2$ arcs which are identified in pairs, and there are exclusively parabolic vertices which are at rational points on the real axis and at ∞.

A transformation in $H(p)$ that has a rational point r/s fixed, where

$(r, s) = 1$, must be of the form

$$\frac{(1 - \nu prs)\tau + \nu pr^2}{-\nu ps^2\tau + 1 + \nu prs}, \tag{14}$$

where ν is even in case rs is even, while ν is any integer in case rs is odd. For if $(\alpha\tau + \beta)/(\gamma\tau + \delta) \in H(p)$ and has r/s fixed, then

$$(\alpha - \rho)r + \beta s = 0, \qquad \gamma r + (\delta - \rho)s = 0, \tag{15}$$

where ρ is rational. The determinant of these equations is

$$\rho^2 - \rho(\alpha + \delta) + 1 = 0,$$

so $\rho = \pm 1$. Without loss of generality take $\rho = 1$. Then

$$\alpha + \delta = 2.$$

Since $\alpha - 1 = -(\delta - 1)$, equations (15) show that the transformation is of the form (14).

This shows that any such transformation belonging to $H(p)$ must belong to $\Gamma(p)$. It also shows that the local uniformizer t in $D_\Gamma(p)$ may be taken

$$t = \begin{cases} e^{-2\pi i/ps(s\tau - r)} & \text{if } rs \text{ is odd,} \\ e^{-i\pi/ps(s\tau - r)} & \text{if } rs \text{ is even.} \end{cases} \tag{16}$$

(Here and henceforth we suppose that $(r, s) = 1$ without explicitly stating so each time.) For let

$$\zeta = \frac{(1 - \nu prs)\tau + \nu pr^2}{-\nu ps^2\tau + 1 + \nu prs}.$$

If

$$\omega = \frac{-1}{\tau - r/s},$$

then

$$\frac{-1}{\zeta - r/s} = \omega + \nu ps^2.$$

Let $\nu = 2$ if rs is even, and $\nu = 1$ if rs is odd. Then t is as given in (16).

Two rational points r/s and r'/s' where $(r, s) = (r', s') = 1$ belong to the same cycle of $D_H(p)$ if and only if the following two conditions are satisfied:

$$(s, p) = (s', p), \qquad rs \equiv r's' \pmod{2p}. \tag{17}$$

For if $(\alpha\tau + \beta)/(\gamma\tau + \delta)$ belongs to $H(p)$ and maps r/s onto r'/s', then

$$\alpha r + \beta s = \rho r', \qquad \gamma r + \delta s = \rho s', \tag{18}$$

where $\rho = \pm 1$. Then

$$r's' \equiv (\alpha r + \beta s)(\gamma r + \delta s) \equiv rs \pmod{2p},$$

and conditions (17) are necessary. For the converse it is sufficient to show that under conditions (17) the points r/s and r'/s' can be mapped into the same point. Thus consider the following cases:

(i) If $(s, p) = p$ and rs is odd, let $xr + 2psy = 1$. Then

$$(x\tau + 2py)/(\gamma\tau + \delta)$$

belongs to $H(p)$ for some γ, δ, and it maps r/s onto $1/kp$ where k is odd. Then $\tau/(2\nu p\tau + 1)$ belongs to $H(p)$, and for some ν it maps $1/kp$ onto $1/p$.

(ii) If $(s, p) = p$ and rs is even, then $(\alpha\tau + \beta)/(-s\tau + r)$ belongs to $H(p)$ for some α, β, and it maps r/s onto ∞.

(iii) If $(s, p) = 1$ let $xpr + \delta s = 1$ where δ or x is even. Then

$$(\alpha\tau + \beta)/(xp\tau + \delta)$$

belongs to $H(p)$ for some α, β, and it maps r/s onto ν. Then, by translation, take $0 \leqq \nu < 2p$. Since conditions (17) have been proved necessary,

$$\nu \equiv rs \pmod{2p}.$$

The parabolic vertices of $D_H(p)$ thus fall into $2p + 2$ cycles which can be represented by the points

$$(19) \qquad \infty,\ 1/p,\ 0,\ 1,\ 2,\ 3,\ \cdots,\ 2p - 1.$$

Two points r/s and r'/s' where $(r, s) = (r', s') = 1$ belong to the same cycle of $D_\Gamma(p)$ if and only if the following conditions are satisfied:

$$(20) \qquad r \equiv \mu r' \pmod{p}, \qquad s \equiv \mu s' \pmod{p}, \qquad rs \equiv r's' \pmod{2},$$

where $\mu = \pm 1$. For since $\alpha \equiv \delta \equiv \pm 1 \pmod{p}$, relations (18) show that conditions (20) are necessary. Conversely, if conditions (20) are satisfied, then conditions (17) are also satisfied, so there is a transformation

$$(\alpha\tau + \beta)/(\gamma\tau + \delta)$$

belonging to $H(p)$ which maps r/s onto r'/s'. But this transformation must belong to $\Gamma(p)$, for (18) and (20) show that, modulo p,

$$\rho r' \equiv \alpha r \equiv \alpha\mu r', \qquad \rho s' \equiv \delta s \equiv \delta\mu s'.$$

Since either r' or s' is relatively prime to p, it follows that α or δ is congruent to ± 1 modulo p. But $\alpha\delta \equiv 1 \pmod{p}$ since the transformation is in $H(p)$, and it follows that $\alpha \equiv \delta \equiv \pm 1 \pmod{p}$. Thus the transformation belongs to $\Gamma(p)$.

It may be shown from (20) that the parabolic vertices of $D_\Gamma(p)$ fall into $p^2 - 1$ cycles. Or one can show that corresponding to each vertex (19) there are $(p - 1)/2$ vertices of $D_\Gamma(p)$ which are in distinct cycles in $D_\Gamma(p)$. Let

$$V_1,\ V_2,\ \cdots,\ V_{(p-1)/2}$$

be cosets of $\Gamma(p)$ in $H(p)$. Every rational number r/s can be mapped by

$\Gamma(p)$ onto one and only one of the $p^2 - 1$ points

$$V_j(v)$$

where $1 \leqq j \leqq (p-1)/2$ and v is one of the vertices (19). For let N be a transformation in $H(p)$ which maps r/s onto a vertex v of (19). Then

$$V_j N \epsilon \Gamma(p)$$

for some j since $\Gamma(p)$ is a normal subgroup of $H(p)$, and $V_j N$ maps r/s onto $V_j(v)$. On the other hand, suppose v_1, v_2 are vertices in the set (19), possibly the same vertex, and suppose there is a transformation $W \epsilon \Gamma(p)$ which maps $V_j(v_1)$ onto $V_k(v_2)$. Then

$$WV_j(v_1) = V_k(v_2)$$

implies that

$$V_k^{-1}WV_j(v_1) = v_2 .$$

Now $V_k^{-1}WV_j \epsilon H(p)$, but distinct vertices (19) belong to distinct cycles of $D_H(p)$. It follows that $v_1 = v_2$. Then $V_k^{-1}WV_j$ has v_1 as a fixed point and must then be of the form (14). Hence this transformation belongs to $\Gamma(p)$. Since $\Gamma(p)$ is a normal subgroup of $H(p)$, the condition $1 \leqq j, k \leqq (p-1)/2$ implies that $j = k$.

The genus g_H of $D_H(p)$ is

$$g_H = \begin{cases} (p^2 - 3p)/4 & \text{if } p \equiv 3 \pmod 4, \\ (p^2 - 3p - 2)/4 & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

For if $p \equiv 3 \pmod 4$, then the boundary of $D_H(p)$ lies on $p^2 + p + 2$ circular arcs which are identified in pairs. There are $p^2 + p + 2$ vertices which fall into $2p + 2$ cycles, each parabolic. If $p \equiv 1 \pmod 4$, then the boundary of $D_H(p)$ consists of $p^2 + p + 4$ circular arcs which are identified in pairs. There are $p^2 + p + 2$ parabolic vertices, which fall into $2p + 2$ cycles, and two elliptic vertices, each of period 2. The genus g_Γ of $D_\Gamma(p)$ is

$$g_\Gamma = (p^3 - 4p^2 - p + 12)/8. \tag{21}$$

For the boundary of $D_\Gamma(p)$ consists of $(p^3 - p + 4)/2$ circular arcs which are identified in pairs. There are $(p^3 - p + 4)/2$ parabolic vertices, which fall into $p^2 - 1$ cycles.

[Referee's remarks. In obtaining (21) the author has used the relationship

$$g = \tfrac{1}{2}(n - k + 1),$$

where g is the genus of a subgroup of the modular group whose fundamental domain, before corresponding sides and vertices are identified, is simply connected and contains $2n$ sides identified in pairs and k cycles of vertices. A different approach to the determination of the genus of the group $\Gamma(p)$ is as follows.

Let $G(n)$ be the principal congruence subgroup of level n of the full modular group. G Then it is known [cf. F. Klein and R. Fricke, *Vorlesungen über die Theorie der elliptischen Modulfunktionen*, vol. 2, p. 654, Leipzig (1892) and E. Hecke, *Zur Theorie der elliptischen Modulfunktionen*, Math. Ann., vol. 97 (1926), pp. 210–242] that the genus g of $G(n)$ is given by

$$g = 1 + \frac{\mu(n - 6)}{12n},$$

where μ is the index of $G(n)$ in G. For $n > 2$, μ is given by

$$\mu = \tfrac{1}{2}n^3 \prod_{p \mid n} \left(1 - \frac{1}{p^2}\right)$$

(here a matrix and its negative are identified). When n is an odd prime p, this gives

$$\mu = \tfrac{1}{2}p(p^2 - 1)$$

and consequently

$$g = (p + 2)(p - 3)(p - 5)/24 = (p^3 - 6p^2 - p + 30)/24.$$

Further, the shape of the fundamental region of $G(p)$ has been fully described.

Now $\Gamma(p)$ is a subgroup of $G(p)$ of index 3, and for a set of right coset representatives for $G(p)$ modulo $\Gamma(p)$ we may choose, for example,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 + p^2 & p \\ p & 1 \end{pmatrix}.$$

Thus the fundamental domain of $\Gamma(p)$ consists of three copies of the fundamental domain of $G(p)$ by the representatives above, and the calculation of the genus of $\Gamma(p)$ can be carried through on this basis.]

III. The functions

In this section certain modular functions are defined, it is shown how they transform under $H(1)$, and their expansion about rational points is determined. Part of this is known; equations (23), (24) were obtained by Kloosterman [7, 8] using the method of Hermite, but I do not know where to find all that will be required. The starting point is the Poisson summation formula

$$\sum_{-\infty}^{\infty} q(n) = \sum_{-\infty}^{\infty} \int_{-\infty}^{\infty} q(t) e^{2\pi i n t}\, dt.$$

This formula is valid, for example, if $q(t)$ is absolutely integrable and $\sum q(t + u)$ has a derivative at $t = 0$.

If λ, μ, a, N are real numbers with $N > 0$, then

$$g(z, \tau) = \sum_{n=-\infty}^{\infty} e^{i\pi N\lambda(n+a)}\, e^{(i\pi\tau/N)(a+\mu N/2+nN)^2}\, e^{2\pi i(a+\mu N/2+nN)z}$$

is a regular function of τ in $\mathrm{Im}(\tau) > 0$ for every finite z, and it satisfies

$$g\left(\frac{z}{\tau}, \frac{-1}{\tau}\right) = \left(\frac{-i\tau}{N}\right)^{1/2} e^{i\pi N z^2/\tau}\, e^{i\pi N\lambda a} \cdot \sum_{-\infty}^{\infty} e^{-(2\pi i/N)(a+\mu N/2)(n+\lambda N/2)}\, e^{(i\pi\tau/N)(n+\lambda N/2)^2}\, e^{2\pi i(n+\lambda N/2)z}. \tag{22}$$

For

$$g\left(\frac{z}{\tau}, \ \frac{-1}{\tau}\right) = \sum_{-\infty}^{\infty} q(n),$$

where

$$q(t) = e^{i\pi\lambda N(t+a)}\, e^{-(i\pi/N\tau)(a+\mu N/2+tN)^2}\, e^{2\pi i(a+\mu N/2+tN)z/\tau}.$$

The Poisson summation formula is valid, and making the successive changes of variable

$$vN = a + \mu N/2 + tN, \qquad u = v - \lambda\tau/2 - n\tau/N - z,$$

we have

$$\int_{-\infty}^{\infty} q(t) e^{2\pi i n t}\, dt = e^{i\pi N z^2/\tau} e^{i\pi\lambda N a} e^{2\pi i z(n+\lambda N/2)} \cdot e^{-(2\pi i/N)(a+\mu N/2)(n+\lambda N/2)}\, e^{(i\pi\tau/N)(n+\lambda N/2)^2} \int_{-\infty}^{\infty} e^{-(i\pi N/\tau)u^2}\, du.$$

Now

$$\int_{-\infty}^{\infty} e^{-(i\pi N/\tau)u^2}\, du = \left(\frac{-i\tau}{N}\right)^{1/2},$$

where the square root has positive real part, so (22) follows.

Now let λ, a be integers, and define

$$f_a(z, \tau, \lambda) = \sum_{-\infty}^{\infty} (-\,1)^{\lambda(n+a)}\, e^{(i\pi\tau/p)(a+\lambda p/2+np)^2}\, e^{2\pi i z(a+\lambda p/2+np)},$$

$$\phi(z, \tau, \lambda) = \sum_{-\infty}^{\infty} (-1)^{\lambda n}\, e^{i\pi\tau(\lambda/2+n)^2}\, e^{2\pi i z(\lambda/2+n)}.$$

Then we have

$$f_{a+p}(z, \tau, \lambda) = f_a(z, \tau, \lambda), \qquad f_{-a}(-z, \tau, \lambda) = (-1)^{\lambda} f_a(z, \tau, \lambda),$$
$$f_a(z, \tau + 2\nu, \lambda) = e^{(2\pi i\nu/p)(a+\lambda p/2)^2} f_a(z, \tau, \lambda),$$

and, by (22),

$$f_a\left(\frac{z}{\tau}, \frac{-1}{\tau}, \lambda\right) = \left(\frac{-i\tau}{p}\right)^{1/2} e^{i\pi p z^2/\tau}\, e^{-i\pi\lambda^2 p/2} \sum_{b=0}^{p-1} e^{-2\pi i a b/p}\, f_b(z, \tau, \lambda).$$

Likewise for the function $\phi(z, \tau, \lambda)$ we have

$$\phi(-z, \tau, \lambda) = (-1)^{\lambda}\, \phi(z, \tau, \lambda),$$

$$\phi(z, \tau + 2\nu, \lambda) = e^{i\pi\nu\lambda^2/2}\, \phi(z, \tau, \lambda),$$
$$\phi\left(\frac{z}{\tau}, \frac{-1}{\tau}, \lambda\right) = (-i\tau)^{1/2}\, e^{i\pi z^2/\tau}\, e^{-i\pi\lambda^2/2}\, \phi(z, \tau, \lambda).$$

The object now is to find how the functions $f_a(z, \tau, \lambda)$ transform under a transformation on τ in $H(1)$ with an appropriate corresponding transformation on z. This will be accomplished by finding how the functions

$$h_a(z, \tau) = \frac{f_a(z, \tau, \lambda)}{\phi^p(z, \tau, \lambda)}$$

transform under $H(1)$, then how the functions $\phi(z, \tau, \lambda)$ transform under $H(1)$. The dependence of $h_a(z, \tau)$ on λ is not indicated because it will appear that the rule of transformation of h under $H(1)$ is independent of λ.

Now we have from the preceding,

$$h_{a+p}(z, \tau) = h_a(z, \tau), \qquad h_{-a}(-z, \tau) = h_a(z, \tau),$$
$$h_a(z, \tau + 2\nu) = e^{2\pi i\nu a^2/p}\, h_a(z, \tau),$$
$$h_a\left(\frac{z}{\tau}, \frac{-1}{\tau}\right) = \frac{1}{\sqrt{p}}\, e^{i\pi(p-1)/4}\, \tau^{(1-p)/2} \sum_{b=0}^{p-1} e^{-(2\pi i/p)ab}\, h_b(z, \tau).$$

If $L(\tau) = (\alpha\tau + \beta)/(\gamma\tau + \delta)$ is a transformation belonging to $H(1)$, define

$$h_a \mid L = (\gamma\tau + \delta)^{(p-1)/2} h_a\left(\frac{z}{\gamma\tau + \delta}, \frac{\alpha\tau + \beta}{\gamma\tau + \delta}\right).$$

It is to be shown that for transformations $L \epsilon H(1)$ we have

$$h_a \mid L = \left(\frac{\delta}{p}\right) e^{\pi i\alpha\beta a^2/p}\, h_{\alpha a}(z, \tau) \tag{23}$$

in case $\gamma \equiv 0 \pmod{p}$, and

$$h_a \mid L = \frac{1}{\sqrt{p}}\left(\frac{\gamma}{p}\right) e^{(i\pi/4)(p-1)} \sum_{b=0}^{p-1} e^{(2\pi i\gamma'/p)(\alpha a^2 - 2ab + \delta b^2)} h_b\,(z, \tau) \tag{24}$$

in case $(\gamma, p) = 1$. Here γ' is defined by $2\gamma\gamma' \equiv 1 \pmod{p}$.

The proof of (23), (24) is by induction. Now (23) is true for the identity. If (23) or (24) is true for a transformation $L \epsilon H(1)$, then it is also true for the transformation $L^*(\tau) = L(\tau + 2\nu)$. If (23) is true for some $L(\tau) \epsilon H(1)$, then writing $L^*(\tau) = L(-1/\tau) = (\beta\tau - \alpha)/(\delta\tau - \gamma)$ we have

$$\begin{aligned} h_a(z, \tau) \mid L^* &= \tau^{(p-1)/2}\left(\frac{\delta}{p}\right) e^{\pi i\alpha\beta a^2/p} h_{\alpha a}\left(\frac{z}{\tau}, \frac{-1}{\tau}\right) \\ &= \frac{1}{\sqrt{p}}\left(\frac{\delta}{p}\right) e^{(i\pi/4)(p-1)} \sum_{b=0}^{p-1} e^{(2\pi i\delta'/p)(\beta a^2 - 2ab - \gamma b^2)} h_b\,(z, \tau), \end{aligned}$$

where $2\delta\delta' \equiv 1 \pmod{p}$. This is (24) for the transformation $L^*(\tau)$.

If (24) is true for $L(\tau)$ belonging to $H(1)$, again writing

$$L^*(\tau) = L(-1/\tau) = (\beta\tau - \alpha)/(\delta\tau - \gamma)$$

we have

$$\begin{aligned} h_a \,|\, L^* &= \tau^{(p-1)/2} \frac{1}{\sqrt{p}} \left(\frac{\gamma}{p}\right) e^{(i\pi/4)(p-1)} \sum_{b=0}^{p-1} e^{(2\pi i\gamma'/p)(\alpha a^2 - 2ab + \delta b^2)} h_b \left(\frac{z}{\tau}, \frac{-1}{\tau}\right) \\ &= \frac{1}{p} \left(\frac{-\gamma}{p}\right) \sum_{c=0}^{p-1} \sum_{b=0}^{p-1} e^{(2\pi i\gamma'/p)(\alpha a^2 - 2ab + \delta b^2)} e^{-(2\pi i/p)bc} h_c(z, \tau). \end{aligned} \tag{25}$$

There are two cases to consider, $\delta \equiv 0 \pmod{p}$ and $\delta \not\equiv 0 \pmod{p}$. In the first case the sum on b is zero unless $c \equiv -2\gamma' a \pmod{p}$. But if $\delta \equiv 0 \pmod{p}$, then $\beta \equiv -2\gamma' \pmod{p}$, so we have

$$h_a \,|\, L^* = \left(\frac{-\gamma}{p}\right) e^{-(\pi i/p)\alpha\beta a^2} h_{\beta a}(z, \tau).$$

This is (23) for the transformation $L^*(\tau)$.

Thus consider the case $(\delta, p) = 1$. For any c define the integer $k = k(c)$ by

$$2\gamma'\delta k \equiv 2\gamma' a + c \qquad \pmod{p}. \tag{26}$$

Then in (25) we have, using a well-known expression for the Gaussian sums

$$\begin{aligned} \sum_{b=0}^{p-1} e^{(2\pi i\gamma'/p)(-2ab + \delta b^2)} e^{-(2\pi i/p)bc} &= \sum_{b=0}^{p-1} e^{(2\pi i\delta\gamma'/p)(b^2 - 2bk)} \\ &= \sqrt{p} \left(\frac{2\delta\gamma'}{p}\right) e^{(i\pi/4)(1-p)} e^{-(2\pi i/p)\delta\gamma' k^2}. \end{aligned}$$

Hence (25) becomes

$$h_a \,|\, L^* = \frac{1}{\sqrt{p}} \left(\frac{\delta}{p}\right) e^{(i\pi/4)(p-1)} \sum_{c=0}^{p-1} e^{(2\pi i\gamma'/p)(\alpha a^2 - \delta k^2)} h_c(z, \tau),$$

where $k = k(c)$ is defined by (26). Let δ' satisfy $2\delta\delta' \equiv 1 \pmod{p}$. Then

$$\begin{aligned} -\gamma'\delta k^2 &\equiv -\gamma\delta'(2\gamma'\delta k)^2 \equiv -\gamma\delta'(2\gamma' a + c)^2 \\ &\equiv \delta'(-2\gamma' a^2 - 2ac - \gamma c^2) \qquad \pmod{p}, \end{aligned}$$

and

$$\gamma'\alpha \equiv \gamma'\alpha 2\delta\delta' \equiv 2\gamma'\delta'(1 + \beta\gamma) \equiv 2\gamma'\delta' + \delta'\beta \qquad \pmod{p}.$$

Thus we have

$$h_a \,|\, L^* = \frac{1}{\sqrt{p}} \left(\frac{\delta}{p}\right) e^{(i\pi/4)(p-1)} \sum_{c=0}^{p-1} e^{(2\pi i\delta'/p)(\beta a^2 - 2ac - \gamma c^2)} h_c(z, \tau)$$

which is (24) for the transformation $(\beta\tau - \alpha)/(\delta\tau - \gamma)$. This completes the induction since the transformations $\tau + 2$ and $-1/\tau$ generate $H(1)$.

Since

$$f_a(z, \tau, \lambda) = h_a(z, \tau)\phi^p(z, \tau, \lambda),$$

the rule of transformation of the functions $f_a(z, \tau, \lambda)$ depends on how the functions $\phi(z, \tau, \lambda)$ transform under this group. It is clear from the definition of $\phi(z, \tau, \lambda)$ that

$$\phi(0, \tau, 0) = \vartheta(\tau) = \sum_{-\infty}^{\infty} e^{i\pi n^2\tau}.$$

The transformation of $\phi(z, \tau, \lambda)$ under $H(1)$ can be inferred from the rule of transformation of $\vartheta(\tau)$ under $H(1)$.

For this purpose define

$$q(z, \tau, \lambda) = \frac{\phi(z, \tau, \lambda)}{\vartheta(\tau)}.$$

Then

$$q(z, \tau + 2\nu, \lambda) = e^{i\pi\nu\lambda^2/2}q(z, \tau, \lambda), \qquad q(-z, \tau, \lambda) = (-1)^{\lambda}q(z, \tau, \lambda),$$

$$q\left(\frac{z}{\tau}, \frac{-1}{\tau}, \lambda\right) = e^{i\pi z^2/\tau}e^{-i\pi\lambda^2/2}q(z, \tau, \lambda).$$

If $(\alpha\tau + \beta)/(\gamma\tau + \delta) \epsilon H(1)$, then

$$q\left(\frac{z}{\gamma\tau + \delta}, \frac{\alpha\tau + \beta}{\gamma\tau + \delta}, \lambda\right) = \eta e^{i\pi z^2\gamma/(\gamma\tau+\delta)}q(z, \tau, \lambda), \tag{27}$$

where

$$\eta = \begin{cases} e^{(i\pi/4)(\beta\delta-\gamma\delta+2\delta-2)\lambda^2} & \text{if } \beta, \gamma \text{ are even,} \\ e^{(i\pi/4)(\alpha\gamma+\gamma\delta+2\gamma-4)\lambda^2} & \text{if } \alpha, \delta \text{ are even.} \end{cases} \tag{28}$$

Relation (27) may be proved by induction, since if it is true for some transformation belonging to $H(1)$ then it remains true when z, τ are replaced by z, $\tau + 2\nu$ or by z/τ, $-1/\tau$. It is clear that (27) holds for the identity, so it holds in general.

We have

$$f_a(z, \tau, \lambda) = h_a(z, \tau)q^p(z, \tau, \lambda)\vartheta^p(\tau),$$

so the transformation of f_a under $H(1)$ is determined by the transformation of h_a, q, ϑ under that group. If $L = (\alpha\tau + \beta)/(\gamma\tau + \delta)\epsilon H(1)$, then, collecting results, we have

$$f_a\left(\frac{z}{\gamma\tau + \delta}, \frac{\alpha\tau + \beta}{\gamma\tau + \delta}, \lambda\right) \tag{29}$$
$$= (h_a | L)\eta^p e^{i\pi z^2 p\gamma/(\gamma\tau+\delta)}q^p(z, \tau, \lambda)S^p(\gamma\tau + \delta)^{1/2}\vartheta^p(\tau),$$

where S is defined by (5). The expansion of $h_a \mid L$ in terms of functions $h_b(z, \tau, \lambda)$ is given by equations (23), (24).

Now let z approach zero, and henceforth write

$$f_a(\tau, \lambda) = \sum_{-\infty}^{\infty} (-1)^{\lambda(n+a)} e^{(i\pi\tau/p)(a+\lambda p/2+np)^2} \tag{30}$$

in place of $f_a(0, \tau, \lambda)$. If λ is odd, then $\phi(0, \tau, \lambda)$ vanishes identically in τ, so $q(0, \tau, \lambda)$ also vanishes when λ is odd. These functions are of course cancelled from the right-hand side of (29) before letting z approach zero. Then (23), (24), (29) show that if $(\alpha\tau + \beta)/(\gamma\tau + \delta) \in H(1)$, then

$$f_a\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}, \lambda\right) = R_1(\gamma\tau+\delta)^{1/2} e^{(i\pi\alpha\beta/p)a^2} f_{\alpha a}(\tau, \lambda) \tag{31}$$

if $\gamma \equiv 0 \pmod{p}$, and

$$f_a\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}, \lambda\right) = R_2\,(\gamma\tau+\delta)^{1/2} \sum_{b=0}^{p-1} e^{(2\pi i\gamma'/p)(\alpha a^2-2ab+\delta b^2)} f_b(\tau, \gamma) \tag{32}$$

if $(\gamma, p) = 1$, where $2\gamma\gamma' \equiv 1 \pmod{p}$. Here

$$R_1 = \left(\frac{\delta}{p}\right) \eta^p S^p, \tag{33}$$

$$R_2 = \frac{1}{\sqrt{p}} \left(\frac{\gamma}{p}\right) e^{(i\pi/4)(p-1)} \eta^p S^p, \tag{34}$$

and

$$\eta = \begin{cases} e^{(i\pi/4)(\beta\delta-\gamma\delta+2\delta-2)\lambda^2} & \text{if} \quad \beta, \gamma \text{ are even,} \\ e^{(i\pi/4)(\alpha\gamma+\gamma\delta+2\gamma-4)\lambda^2} & \text{if} \quad \alpha, \delta \text{ are even,} \end{cases} \tag{35}$$

$$S = \begin{cases} \left(\frac{\gamma}{\delta}\right) e^{(i\pi/4)(\delta-1)} & \text{if} \quad \beta, \gamma \text{ are even,} \quad \delta > 0, \\ \left(\frac{\delta}{\gamma}\right) e^{-(i\pi/4)\gamma} & \text{if} \quad \alpha, \delta \text{ are even,} \quad \gamma > 0. \end{cases} \tag{36}$$

Having determined in (31) (32) the transformation of the functions $f_a(\tau, \lambda)$ in $H(1)$, we now find their expansion about rational points r/s. Now every rational point can be mapped by transformations belonging to $H(1)$ into $\tau = 1$ or $\tau = \infty$. Thus the expansion of a function $f_a(\tau, \lambda)$ near any rational number can be referred to an expansion near 1 or ∞. In order to find the expansion of $f_a(\tau, \lambda)$ near $\tau = 1$ write (30) in the form

$$f_a\left(\frac{\tau-1}{\tau}, \lambda\right) = e^{(i\pi/p)a^2}\, e^{i\pi\lambda^2 p/4}\, (-1)^a \sum_{-\infty}^{\infty} (-1)^{n+a}\, e^{-(i\pi/p\tau)(a+\lambda p/2+np^2)}.$$

Then, using (22), it follows that

$$f_a\left(\frac{\tau - 1}{\tau}, \lambda\right) = e^{(i\pi/p)a^2}\, e^{i\pi\lambda^2 p/4} \left(\frac{-i\tau}{p}\right)^{1/2} \sum_{-\infty}^{\infty} e^{-(2\pi i/p)(a+\lambda p/2)(n+p/2)}\, e^{(i\pi\tau/p)(n+p/2)^2}.$$

Then, replacing τ by $-1/(\tau - 1)$, we have

$$\begin{aligned} f_a(\tau, \lambda) &= \left\{\frac{i}{p(\tau - 1)}\right\}^{1/2} e^{(i\pi/p)a^2} e^{i\pi\lambda^2 p/4} \\ &\quad \cdot \sum_{-\infty}^{\infty} e^{-(2\pi i/p)(a+\lambda p/2)(n+p/2)} e^{-(i\pi/p(\tau-1))(n+p/2)^2}. \end{aligned} \tag{37}$$

Thus the definition (30) of $f_a(\tau, \lambda)$ and equation (37) give the expansion of $f_a(\tau, \lambda)$ in the neighborhood of ∞ and 1 respectively. It will be convenient to write equations (31), (32) in the form

$$f_a(\tau, \lambda) = R_1 \left(\frac{1}{-\gamma\tau + \alpha}\right)^{1/2} e^{(i\pi\alpha\beta/p)a^2} f_{\alpha a}\left(\frac{\delta\tau - \beta}{-\gamma\tau + \alpha}, \lambda\right) \tag{38}$$

if $\gamma \equiv 0 \pmod{p}$, and

$$f_a(\tau, \lambda) = R_2 \left(\frac{1}{-\gamma\tau + \alpha}\right)^{1/2} \sum_{b=0}^{p-1} e^{(2\pi i\gamma'/p)(\alpha a^2 - 2ab + \delta b^2)} f_b\left(\frac{\delta\tau - \beta}{-\gamma\tau + \alpha}, \lambda\right) \tag{39}$$

if $(\gamma, p) = 1$, where $2\gamma\gamma' \equiv 1 \pmod{p}$.

To find the expansion of $f_a(\tau, \lambda)$ about a vertex r/s we suppose $(r, s) = 1$ and $s > 0$. Let u be the local uniformizer, and consider the following cases.

(i) If rs is even and $(s, p) = 1$, choose β, δ such that

$$(r\tau + \beta)/(s\tau + \delta) \,\epsilon\, H(1)$$

with $\delta > 0$. Then by substituting the series for $f_b((\delta\tau - \beta)/(-s\tau + r), \lambda)$ defined by (30) into the right-hand side of (39) we obtain

$$f_a(\tau, \lambda) = \frac{R_2}{(-s\tau + r)^{1/2}} \sum_{-\infty}^{\infty} (-1)^{\lambda m} e^{(2\pi i s'/p)(ra^2 - 2am + \delta m^2)} u^{(m+\lambda p/2)^2}, \tag{40}$$

where

$$u = e^{-i\pi\delta/ps} e^{-i\pi/ps(s\tau - r)}$$

and $2ss' \equiv 1 \pmod{p}$.

(ii) If rs is even and $p \mid s$, let $(r\tau + \beta)/(s\tau + \delta) \,\epsilon\, H(1)$ with $\delta > 0$. Then by (30), (38) we have

$$f_a(\tau, \lambda) = \frac{R_1}{(-s\tau + r)^{1/2}} e^{(i\pi r\beta/p)a^2} \sum_{-\infty}^{\infty} (-1)^{\lambda(n+ra)} u^{(ra+\lambda p/2+np)^2}, \tag{41}$$

where

$$u = e^{-i\pi\delta/ps} e^{-i\pi/ps(s\tau - r)}.$$

(iii) If rs is odd and $(p, s) = 1$, we define a transformation

$$(\delta\tau - \beta)/(-\gamma\tau + \alpha)$$

which belongs to $H(1)$ and maps r/s onto $\tau = 1$. For this purpose let β, δ satisfy $\delta r - \beta s = 1$ and define $\alpha = r - \beta$, $\gamma = s - \delta$. This determines δ only in a residue class modulo s, so let δ be such that $\gamma \equiv 0 \pmod{2p}$ and $\delta > 0$. Then $(\alpha\tau + \beta)/(\gamma\tau + \delta) \epsilon H(1)$, and from (38) and (37) we have after some simplification

$$\begin{aligned} f_a(\tau, \lambda) &= \frac{R_1}{\sqrt{p}} \left(\frac{i}{s\tau - r}\right)^{1/2} e^{(i\pi\alpha r/p)a^2} e^{(i\pi/4)\lambda^2 p} \\ &\qquad \cdot \sum_{-\infty}^{\infty} e^{-(2\pi i/p)(\alpha a + \lambda p/2)(n+p/2)} u^{(2n+p)^2/8}, \end{aligned} \tag{42}$$

where

$$u = e^{2\pi i\gamma/ps} e^{-2\pi i/ps(s\tau - r)}.$$

(iv) If rs is odd and $p \mid s$, let $\delta r - \beta s = 1$ and define $\alpha = r - \beta$, $\gamma = s - \delta$. Choose δ such that γ is even and $\delta > 0$. Then $(\alpha\tau + \beta)/(\gamma\tau + \delta) \epsilon H(1)$, and since $(\gamma, p) = 1$ we use (37) and (39). These give

$$\begin{aligned} f_a(\tau, \lambda) = \frac{R_2}{\sqrt{p}} \left(\frac{i}{s\tau - r}\right)^{1/2} e^{i\pi\lambda^2 p/4} \sum_{b=0}^{p-1} \sum_{n=-\infty}^{\infty} e^{(2\pi i\gamma'/p)(\alpha a^2 - 2ab + \delta b^2)} \\ \cdot e^{(i\pi/p)b^2} e^{-(2\pi i/p)(b + \lambda p/2)(n+p/2)} u^{(2n+p)^2/8}, \end{aligned}$$

where

$$u = e^{2\pi i\gamma/ps} e^{-2\pi i/ps(s\tau - r)}.$$

In order to simplify we sum first on b, noting first that

$$2\gamma'\delta + 1 \equiv 2\gamma'(s - \gamma) + 1 \equiv -2\gamma'\gamma + 1 \equiv 0 \pmod{p}.$$

The sum on b is thus

$$\sum_{b=0}^{p-1} e^{\pi i b^2} e^{(\pi i/p)b(-4a\gamma' - 2n - p)} = \sum_{b=0}^{p-1} e^{-(2\pi i/p)(2a\gamma' + n)b},$$

which is zero unless $2a\gamma' + n \equiv 0 \pmod{p}$. The congruences $2\gamma\gamma' \equiv 1$, $\gamma \equiv -\delta$, $\delta r \equiv 1 \pmod{p}$ imply that $2\gamma' \equiv -r \pmod{p}$. Thus writing $n = ar + mp$ we have

$$f_a(\tau, \lambda) = \frac{Q(-1)^a e^{-i\pi\alpha r a^2/p}}{\sqrt{s\tau - r}} \sum_{-\infty}^{\infty} (-1)^{\lambda(a+m)} u^{(2ar+p+2mp)^2/8}, \tag{43}$$

where

$$Q = \sqrt{p}\, R_2\, e^{(i\pi/4)(\lambda^2 p - 2\lambda p + 1)}.$$

Thus the expansion of the functions $f_a(\tau, \lambda)$ near rational points has been determined. There remains the function

$$\phi(\tau) = \vartheta(\tau/p).$$

But from (3) and (30) it follows that

$$\phi(\tau) = f_0(\tau/p^2, 0)$$

so the expansions for $\phi(\tau)$ can be obtained from the preceding. It will be sufficient for our purpose to find the order of the zeros of the function

$$(s\tau - r)^{1/2}\phi(\tau)$$

at the rational points. If τ approaches r/s, the variable τ/p^2 approaches

$$r/p^2 s = R/S,$$

where $(R, S) = 1$. In case rs is even, it follows from (40), (41) that the function $(s\tau - r)^{1/2}\phi(\tau)$ is regular and not zero at r/s. If rs is odd and $(p, r) = 1$, then $S = p^2 s$, so (43) shows that

$$(s\tau - r)^{1/2}\phi(\tau) = u^{1/8}\{a_0 + \cdots\}$$

near $\tau = r/s$ where $a_0 \neq 0$ and u is the local uniformizer. If rs is odd and $p \mid r$, then (42), (43) show that $(s\tau - r)^{1/2}\phi(\tau)$ has a zero of order $p^2/8$ at $\tau = r/s$, that is,

$$(s\tau - r)^{1/2}\phi(\tau) = u^{p^2/8}\{a_0 + \cdots\},$$

where $a_0 \neq 0$ and u is the local uniformizer.

We now find that the total number of zeros of the functions $(s\tau - r)^{1/2} f_a(\tau, \lambda)$ at the vertices of the fundamental domain $D_\Gamma(p)$. According to (20) the vertices

$$\nu/p, \qquad 0 < \nu < p,$$

belong to different cycles of $D_\Gamma(p)$, and every vertex r/s where $p \mid s$ can be mapped by $\Gamma(p)$ into one of them. The $(p - 1)/2$ vertices with ν odd correspond to the cycle $1/p$ of $D_H(p)$, while the $(p - 1)/2$ vertices with ν even correspond to the cycle ∞ in $D_H(p)$. Each of the vertices

$$0, \ 1, \ 2, \ \cdots, \ 2p - 1$$

of $D_H(p)$ corresponds to $(p - 1)/2$ distinct cycles of $D_\Gamma(p)$ at vertices r/s, $(p, s) = 1$, and at the $(p - 1)/2$ cycles r/s of $D_\Gamma(p)$ corresponding to the cycle κ of $D_H(p)$ we have $\kappa \equiv rs \pmod 2$. Thus there are $(p^2 - p)/2$ cycles r/s in $D_\Gamma(p)$ in which rs is even and $(s, p) = 1$, and the same number of cycles for which rs is odd and $(s, p) = 1$. The following table gives the order of the zeros of the functions $(s\tau - r)^{1/2} f_a(\tau, \lambda)$ and $(s\tau - r)^{1/2}\phi(\tau)$ at the various vertices.

	r/p, r odd	r/p, r even	r/s, rs odd, $(s, p) = 1$	r/s, rs even, $(s, p) = 1$
$f_a(\tau, 0)$	$\frac{1}{8}(2ra + p + 2np)^2$	$(ra + np)^2$	$\frac{1}{8}$	0
$f_a(\tau, 1)$	$\frac{1}{8}(2ra + p + 2np)^2$	$\frac{1}{4}(2ra + p + 2np)^2$	$\frac{1}{8}$	$\frac{1}{4}$
$\phi(\tau)$	$\frac{1}{8}$	0	$\frac{1}{8}$ if $(p, r) = 1$, $p^2/8$ if $p \mid r$	0

In each case n is to be chosen so as to minimize the term in which it occurs. Also $a \not\equiv 0 \pmod{p}$ in the case of the function $f_a(\tau, 1)$. In the case of the vertices r/p we have $0 < r < p$.

Then it follows that for each of the functions $f_a(\tau, 0), f_a(\tau, 1), \phi(\tau)$ we obtain $(p^3 - p)/16$ zeros at the vertices of $D_\Gamma(p)$. For consider a function $f_a(\tau, 0)$ where $a \not\equiv 0 \pmod{p}$. At the vertices r/p, where r is odd, $0 < r < p$, write

$$2ra + p + 2np = \kappa_r, \qquad -p < \kappa_r < p.$$

Then κ_r is odd, and $\kappa_r^2/8$ is the order of the zero at this vertex. The numbers κ_r^2 are distinct, for if there were another vertex r_1/p in this set such that

$$2r_1 a + p + 2n_1 p = \pm\kappa_r$$

then $r_1 \pm r \equiv 0 \pmod{p}, r = r_1$. Thus the total order of zeros at the vertices r/p, r odd, $0 < r < p$, is

$$\tfrac{1}{8}\{1^2 + 3^2 + 5^2 + \cdots + (p-2)^2\} = p(p-1)(p-2)/48.$$

For the vertices r/p where r is even, $0 < r < p$, write

$$ra + np = \nu_r, \qquad -p/2 < \nu_r < p/2.$$

Then the order of the zero is ν_r^2, and one shows that the $(p-1)/2$ numbers ν_r^2 are distinct and $\nu_r \neq 0$. Thus the total order of the zeros at these vertices is

$$1^2 + 2^2 + 3^2 + \cdots + ((p-1)/2)^2 = p(p^2-1)/24.$$

Thus for the function $f_a(\tau, 0)$ where $a \not\equiv 0 \pmod{p}$ the total order of zeros at all parabolic vertices is

$$p(p-1)(p-2)/48 + p(p^2-1)/24 + (p^2-p)/16 = (p^3-p)/16,$$

and likewise for the functions $f_0(\tau, 0), f_a(\tau, 1), \phi(\tau)$.

Now

$$f_0(\tau, 0) = \vartheta(p\tau), \qquad \phi(\tau) = \vartheta\left(\frac{\tau}{p}\right).$$

It can be shown by considering the integral

$$\frac{1}{2\pi i}\int \frac{\vartheta'(\tau)}{\vartheta(\tau)}\, d\tau$$

around the fundamental domain of the group $H(1)$ that the only zeros of $\vartheta(\tau)$ in the fundamental domain of $H(1)$ are at the vertices $\tau = \pm 1$. [Referee's remark. This is evident also from the infinite product

$$\vartheta(\tau) = \prod_{n=1}^{\infty}\{(1 - e^{\pi i(\tau+1)n})(1 + e^{\pi i(\tau+1)n})^{-1}\}.]$$

Thus $\vartheta(\tau)$ has no zero in $\operatorname{Im}(\tau) > 0$, and so $f_0(\tau, 0)$ has no zero in $\operatorname{Im}(\tau) > 0$. But (31) shows that the function $f_a(\tau, 0)/f_0(\tau, 0)$ is automorphic under the group $\Gamma(p)$, so $f_a(\tau, 0)$ and $f_0(\tau, 0)$ have the same number of zeros in $D_\Gamma(p)$. Thus $f_a(\tau, 0)$ has no zeros in $D_\Gamma(p)$ except those at the parabolic vertices.

The function

$$\left\{\frac{f_a(\tau, 1)}{f_0(\tau, 0)}\right\}^8$$

is automorphic under the group $\Gamma(p)$, so $f_a(\tau, 1)$ has the same number of zeros in $D_\Gamma(p)$ as does $f_0(\tau, 0)$. Thus the only zeros of $f_a(\tau, 1)$ in $D_\Gamma(p)$ are at the vertices. This could also be proved by considering the representation of $f_a(\tau, \lambda)$ as an infinite product.

IV. The divisors

We prove first that the functions $\psi(\tau, \chi)$ defined by (1) transform in $H(p)$ according to (8), where $\chi(n)$ is a Dirichlet character function modulo p with $\chi(-1) = 1$. For this purpose we note that

$$\psi(\tau, \chi) = \sum_{a=1}^{p-1} \chi(a) f_a(\tau, 0) = 2 \sum_{a=1}^{(p-1)/2} \chi(a) f_a(\tau, 0).$$

Then (31) shows that for transformations in $H(p)$ we have

$$\psi\left(\frac{\alpha\tau + \beta}{\gamma\tau + \delta}, \chi\right) = R_1(\gamma\tau + \delta)^{1/2}\chi(\delta)\psi(\tau, \chi).$$

But $R_1 = S'$ for transformations in $H(p)$ if λ is even, so (8) follows.

The functions $\psi(\tau, \chi)/\phi(\tau)$ where $\chi(-1) = 1$ are automorphic under $\Gamma(p)$. Each of them has a pole of order $(p^2 - 1)/8$ at each of the cycles

$$(44) \qquad p/s, \qquad s = 1, 3, 5 \cdots, (p-2).$$

Thus let Q' be a divisor which has poles of order $(p^2 - 1)/8$ at each of these $(p-1)/2$ cycles. Then the $(p+1)/2$ functions $\phi(\tau)$, $\psi(\tau, \chi)$ are a complete set of linearly independent functions satisfying (9), (10) if and only if the $(p+1)/2$ functions 1, $\psi(\tau, \chi)/\phi(\tau)$ are a complete set of linearly independent multiples of Q'.

The order $|Q'|$ of Q' is $(p^2 - 1)(p - 1)/16$ which, when $p > 3$, is less than $2g - 1$, where

$$g = (p^3 - 4p^2 - p + 12)/8$$

is the genus of $D_\Gamma(p)$. To define a divisor Q of order $|Q| \geqq 2g - 1$, first note that the functions

$$(45) \qquad F_a(\tau) = \frac{f_a(\tau, 1)}{f_1(\tau, 1)}, \qquad 1 \leqq a \leqq p - 1,$$

are automorphic under $\Gamma(p)$. The poles of these functions lie at the cycles

$$(46) \qquad r/p, \qquad r = 1, 2, 3, \cdots, (p-1).$$

Now $f_1(\tau, 1)$ has zeros of total multiplicity $(p^3 - 3p^2 + 2p)/16$ at these cycles. At each of the cycles r/p there is an a such that $f_a(\tau, 1)$ has a zero of precise order $\frac{1}{8}$ in case r is odd, and a zero of precise order $\frac{1}{4}$ in case r is even. Thus all the functions $F_a(\tau)$ are multiples of a divisor having poles at the vertices (46) of total multiplicity

$$\tfrac{1}{16}(p^3 - 3p^2 - p + 3).$$

Define

$$\sigma_a(\tau) = \frac{f_a(\tau, 0)}{\phi(\tau)}, \qquad 1 \leqq a \leqq (p - 1)/2,$$

and write

$$\sigma_0(\tau) = 1.$$

Then the functions $\sigma_a(\tau)$ are multiples of a divisor having poles of order $(p^2 - 1)/8$ at each of the vertices (44). This divisor then has poles of total multiplicity

$$\tfrac{1}{16}(p^2 - 1)(p - 1).$$

Now consider the functions

$$(47) \quad F_a(\tau)F_b(\tau)\sigma_c(\tau), \quad 1 \leqq a \leqq b \leqq (p - 1)/2, \quad 0 \leqq c \leqq (p - 1)/2,$$

and

$$(48) \quad F_a(\tau)\sigma_b(\tau)\sigma_c(\tau), \quad 1 \leqq a \leqq (p -1)/2, \quad 0 \leqq b \leqq c \leqq (p - 1)/2.$$

Each of them is automorphic under $\Gamma(p)$, and each is a multiple of a divisor Q which has poles at the vertices (44), (46). The order $| Q |$ of Q is

$$\begin{aligned} | Q | &= \tfrac{1}{8}(p^3 - 3p^2 - p + 3) + \tfrac{1}{8}(p^2 - 1)(p - 1) \\ &= \tfrac{1}{4}(p^3 - 2p^2 - p + 2) = \tfrac{1}{4}(p^2 - 1)(p - 2). \end{aligned}$$

Then $| Q | > 2g - 2$ so it follows from the Riemann-Roch theorem that there are precisely

$$| Q | - g + 1 = (p^3 - p)/8$$

linearly independent multiples of Q.

There are

$$\tfrac{1}{16}(p - 1)(p + 1)^2$$

functions (47), and

$$\tfrac{1}{16}(p - 1)(p + 1)(p + 3)$$

functions (48). However $F_1 = \sigma_0 = 1$, so there are

$$\tfrac{1}{4}(p^2 - 1)$$

functions common to the two sets. The total number of functions (47), (48) is then

$$\tfrac{1}{8}(p^3 - p).$$

If they are linearly independent, then they are a complete set of linearly independent multiples of Q.

The poles of Q' are among the poles of Q, so if there are $(p^3 - p)/8$ linearly independent functions among (47), (48) then the multiples of Q' are linear combinations of the functions (47), (48).

Bibliography

1. Paul T. Bateman, *On the representations of a number as the sum of three squares*, Trans. Amer. Math. Soc., vol. 71 (1951), pp. 70–101.
2. H. Hamburger, *Über die Riemannsche Funktionalgleichung der ζ-Funktion (Erste Mitteilung)*, Math. Zeitschrift, vol. 10 (1921), pp. 240–254.
3. ———, *Über die Riemannsche Funktionalgleichung der ζ-Funktion (Zweite Mitteilung)*, Math. Zeitschrift, vol. 11 (1921), pp. 224–245.
4. ———, *Über die Riemannsche Funktionalgleichung der ζ-Funktion (Dritte Mitteilung). Die Funktionalgleichung der L-Reihen*, Math. Zeitschrift, vol. 13 (1922), pp. 283–311.
5. E. Hecke, *Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung*, Math. Ann., vol. 112 (1936), pp. 664–699.
6. ———, *Herleitung des Euler-Produktes der Zetafunktion und einiger L-Reihen aus ihrer Funktionalgleichung*, Math. Ann., vol. 119 (1944), pp. 266–287.
7. H. D. Kloosterman, *The behavior of general theta functions under the modular group and the characters of binary modular congruence groups. I*, Ann. of Math. (2), vol. 47 (1946), pp. 317–375.
8. ———, *The behavior of general theta functions under the modular group and the characters of binary modular congruence groups. II*, Ann. of Math. (2), vol. 47 (1946), pp. 376–447.
9. Morris Newman, *Structure theorems for modular subgroups*, Duke Math. J., vol. 22 (1955), pp. 25–32.
10. Hans Rademacher, *Trends in research: The analytic number theory*, Bull. Amer. Math. Soc., vol. 48 (1942), pp. 379–401.
11. C. L. Siegel, *Bermerkung zu einem Satz von Hamburger über die Funktionalgleichung der Riemannschen Zetafunktion*, Math. Ann., vol. 86 (1922), pp. 276–279.

University of Wisconsin
Madison, Wisconsin