ACTA ARITHMETICA
LIV (1990)

The construction of modular forms as products of transforms of the Dedekind eta function

by

ANTHONY J. F. BIAGIOLI (Rolla, Mo.)

0. Introduction and statement of results. We let $\boldsymbol{H} = \{\tau \in \boldsymbol{C} |\ \operatorname{Im}\tau > 0\}$ be the upper half-plane. For $\tau \in \boldsymbol{H}$, the Dedekind eta function is defined by

$$\eta(\tau) = x^{1/24}\prod_{n=1}^{\infty}(1-x^n), \tag{0.1}$$

where $x = e^{2\pi i\tau}$ and the power of x is interpreted as $x^{\alpha} = e^{2\pi i\alpha\tau}$. A *transform of level* n of $\eta(\tau)$, in reduced form, is a function of the form

$$h(\tau) = \gamma\cdot\eta\left(\frac{a\tau+b}{d}\right), \tag{0.2}$$

where a, b, and d are positive integers satisfying $ad = n$, $(a, b, d) = 1$, $0 \leqslant b < d$, and γ is a non-zero constant, and by an *eta product* we shall mean a function of the form

$$h(\tau) = \gamma\cdot\prod\eta\left(\frac{a\tau+b}{d}\right)^{\alpha(a,b,d)}, \tag{0.3}$$

where γ is a non-zero constant, each $\alpha(a, b, d)$ is a real number, the product is over the reduced transforms, and there should be only a finite number of factors in the product.

The object of this paper is to investigate the overall limitations, in terms of the orders at the cusps and in terms of multiplicative independence, on the functions which can be constructed as eta products.

Eta products appear in many areas of mathematics in which algebra and analysis overlap, notably, of late, in Lie algebras (cf. Kac [3]) and their applications to the classification of finite simple groups (cf. Conway and Norton [2]). M. Newman published a pair of fairly well-known papers [6], [7] dealing with eta products, but these papers treat only the case $d = 1$, $b = 0$, which we call the *principal transforms*, and are aimed at constructing forms on the groups $\Gamma_0(n)$ which have the trivial multiplier system, whereas we shall pay no attention to the multiplier system, but shall be concerned only with the orders of the resulting eta product at the cusps.

We will now state the principal results of this paper as five theorems, designated by A–E. To state these theorems we need a couple of definitions; a summary of the standard definitions will be given in Section 1. We let $\frac{1}{0} = \infty$ be the point at infinity of $\boldsymbol{C}$, let $\boldsymbol{Q}^* = \boldsymbol{Q} \cup \{\infty\}$, and let $\kappa(\Gamma;\zeta)$ denote the width of the group $\Gamma \subseteq \Gamma(1)$ at the cusp $\zeta \in \boldsymbol{Q}^*$.

DEFINITION 0.1. The *invariant order of a modular form f at a cusp $\zeta \in \boldsymbol{Q}^*$* is

$$\operatorname{ord}(f;\zeta) = \frac{1}{\kappa(\Gamma;\zeta)} \operatorname{Ord}_\Gamma(f;\zeta),$$

where Γ is any subgroup of finite index in $\Gamma(1)$ on which f is a form, and $\operatorname{Ord}_\Gamma(f;\zeta)$ is the standard order of f with respect to Γ at ζ.

DEFINITION 0.2. For any natural number n, we define an equivalence relation on $\boldsymbol{Q}^*$, which we call star-equivalence modulo n, as follows: two elements ζ, $\zeta' \in \boldsymbol{Q}^*$, are *star-equivalent modulo n*, in symbols

$$\zeta *\sim \zeta' \pmod{n},$$

if and only if

$$\operatorname{ord}\left(\eta\left(\frac{a\tau+b}{d}\right);\zeta\right) = \operatorname{ord}\left(\eta\left(\frac{a\tau+b}{d}\right);\zeta'\right)$$

for every transform $\eta\left(\frac{a\tau+b}{d}\right)$ of level n.

The first result is an arithmetic characterization of star-equivalence modulo n.

THEOREM A. *If $n \in \boldsymbol{N}$, and $\frac{r}{s}, \frac{r'}{s'} \in \boldsymbol{Q}^*$, with $(r, s) = (r', s') = 1$, then*

$$\frac{r}{s} *\sim \frac{r'}{s'} \pmod{n}$$

if and only if there is some α relatively prime to n such that

$$\begin{cases} r' \equiv \alpha r \pmod{n}, \\ s' \equiv \alpha s \pmod{n}. \end{cases} \tag{0.4}$$

The next theorem is the multiplicative independence of the transforms of level n.

THEOREM B. *If $\alpha(a, b, d)$ are any real numbers, then*

$$\prod_{ad=n} \prod_{\substack{b=0 \\ (a,b,d)=1}}^{d-1} \eta\left(\frac{a\tau+b}{d}\right)^{\alpha(a,b,d)}$$

is constant if and only if $\alpha(a, b, d) = 0$ for all a, b, d.

We shall then characterize the eta products as follows:

THEOREM C. *Suppose f is a modular form. Then f is an eta product if and only if*
(i) *f has no zeros of poles in $\boldsymbol{H}$, and*
(ii) *for some natural number n the invariant order of f is invariant under star-equivalence, i.e.,*

$$\zeta *\sim \zeta' \pmod{n} \Rightarrow \operatorname{ord}(f;\zeta) = \operatorname{ord}(f;\zeta'). \tag{0.5}$$

For the principal congruence subgroups, $\Gamma(n)$, and the principal transform subgroups, $\Gamma_0(n)$, we describe a multiplicative basis for the family of all eta products which are forms on these groups. For $\Gamma(n)$ the result is quite simple; a basis is the set of transforms of level exactly n.

THEOREM D. *Suppose h is an eta product which is a form on $\Gamma(n)$. Then there are unique real numbers $\alpha(a, b, d)$ for each a, b, d, satisfying $ad = n$, $0 \leqslant b < d$, and $(a, b, d) = 1$, and a non-zero constant γ so that*

$$h(\tau) = \gamma \cdot \prod_{ad=n} \prod_{\substack{0 \leqslant b < d \\ (a,b,d)=1}} \eta\left(\frac{a\tau+b}{d}\right)^{\alpha(a,b,d)}.$$

For $\Gamma_0(n)$ our description of a multiplicative basis is more complicated. Given n, we select a divisor δ of n as follows: First let δ_0 be the largest odd square-free number such that $\delta_0^2 | n$. Then we set

$$\delta = \begin{cases} \delta_0, & \text{if } 16 \nmid n, \\ 4\delta_0, & \text{if } 16 | n \text{ and } 64 \nmid n, \\ 8\delta_0, & \text{if } 64 | n. \end{cases} \tag{0.6}$$

Thus δ can be described as the largest number which has no square divisors other than 1 or 4, such that $\delta^2 | n$, and which satisfies the additional proviso that either $2 \nmid \delta$, or $4 | \delta$. As usual, we write $d \| \delta$ to mean that $d | \delta$ and $(d, \delta/d) = 1$. We can write any $d \| \delta$ in the form $d = 2^\alpha d_0$, where $d_0 \| \delta_0$, and we write $b \sim 1 \pmod{d_0}$ to mean that b is a quadratic residue modulo d_0, i.e., there is some c relatively prime to d_0 such that $b \equiv c^2 \pmod{d_0}$. We then define certain eta products as follows:

$$h_{d,1}(\tau) = \prod_{\substack{0 \leqslant b < d \\ b \sim 1 \pmod{d}}} \eta\left(\tau + \frac{b}{d}\right), \quad \text{for any } d \| \delta,$$

$$h_{d,i}(\tau) = \prod_{\substack{0 \leqslant b < d \\ b \sim 1 \pmod{d_0} \\ b \equiv i \pmod{8}}} \eta\left(\tau + \frac{b}{d}\right), \quad \text{when } d \| \delta,\ 8 | d \text{ and } i = 3, \text{ or } 7. \tag{0.7}$$

Thus, $h_{d,1}$ is defined for any d, but $h_{d,3}$ and $h_{d,7}$ are defined only when $8 | d$. Since the quadratic residues modulo 8 are the numbers congruent to 1 modulo 8, the definition of $h_{d,1}$ can be taken from either equation when $8 | d$.

Some examples of the functions $h_{d,i}(\tau)$ are:

$$h_{3,1}(\tau) = \eta(\tau+\tfrac{1}{3}),$$

$$h_{5,1}(\tau) = \eta(\tau+\tfrac{1}{5})\eta(\tau+\tfrac{4}{5}),$$

$$h_{40,7}(\tau) = \eta(\tau+\tfrac{31}{40})\eta(\tau+\tfrac{39}{40}).$$

The following theorem says that the collection of $h_{d,i}$ for $d \| \delta$ is a multiplicative basis for the eta products which are forms on $\Gamma_0(n)$. Since $h_{1,1}(\tau) = \eta(\tau)$, the functions $\eta(a\tau)$ for $a|n$ are included among the functions $h_{d,i}(a\tau)$, so the principal transforms are in this basis. Sometimes, but not always (cf. the corollary following the theorem), the principal transforms will be the only functions appearing in the basis.

THEOREM E. *Suppose h is an eta product which is a modular form on $\Gamma_0(n)$. Then there are unique real numbers $\beta_i(a, d)$ such that*

$$h(\tau) = \gamma \cdot \prod_{a,d,i} h_{d,i}(a\tau)^{\beta_i(a,d)},$$

where the product runs over those a, d, i such that

$$d \| \delta,$$

$$ad^2 | n,$$

$$i = \begin{cases} 1, & \text{if } 8 \nmid d, \\ 1, 3, \text{ or } 7, & \text{if } 8 | d. \end{cases}$$

COROLLARY. *Every eta product on $\Gamma_0(n)$ can be expressed uniquely in the form*

$$h(\tau) = \prod_{a|n} \eta(a\tau)^{\alpha(a)},$$

where $\alpha(a)$ are real numbers, if and only if n is divisible by no square other than 1 or 4.

EXAMPLE. For $n = 64 \cdot 25$ a multiplicative basis for all of the eta products which are forms on $\Gamma_0(n)$ is

$$h_{1,1}(a\tau) = \eta(a\tau), \qquad \text{for } a|1600,$$

$$h_{8,i}(a\tau) = \eta(a\tau+\tfrac{1}{8}),\ \eta(a\tau+\tfrac{3}{8}),\ \eta(a\tau+\tfrac{7}{8}), \qquad \text{for } a|25,$$

$$h_{5,1}(a\tau) = \eta(a\tau+\tfrac{1}{5})\eta(a\tau+\tfrac{4}{5}), \qquad \text{for } a|64,$$

$$h_{40,i}(\tau) = \eta(\tau+\tfrac{1}{40})\eta(\tau+\tfrac{9}{40}),\ \eta(\tau+\tfrac{11}{40})\eta(\tau+\tfrac{19}{40}),\ \eta(\tau+\tfrac{31}{40})\eta(\tau+\tfrac{39}{40}).$$

1. Definitions and background. As usual, $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, and $\boldsymbol{C}$ shall denote the integers, and the rational, real, and complex numbers, respectively. We let $M_2(\boldsymbol{Z})$ be the set of 2×2 matrices with entries in the integers $\boldsymbol{Z}$, we set

$$M_2^+(\boldsymbol{Z}) = \{M \in M_2(\boldsymbol{Z}) |\ \det(M) > 0\} \quad \text{and} \quad \Gamma(1) = \{M \in M_2(\boldsymbol{Z}) |\ \det(M) = 1\}.$$

For $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2^+(\boldsymbol{Z})$ we define $g = \gcd(M)$ to be the greatest common divisor of a, b, c, and d, and the *level* of M to be

$$\text{lev}(M) = \frac{\det(M)}{g^2}. \tag{1.1}$$

We say M is *primitive* if $\gcd(M) = 1$. We say that M is *reduced* if $c = 0$, $a, d > 0$, and $0 \leqslant b < d$. We denote the set of all primitive reduced matrices in $M_2^+(\boldsymbol{Z})$ by

$$\boldsymbol{T} = \{M \in M_2^+(\boldsymbol{Z}) |\ M \text{ is primitive and reduced}\},$$

and the subset consisting of those whose level is n by

$$\boldsymbol{T}_n = \{M \in \boldsymbol{T} |\ \text{lev}(M) = n\} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle|\ ad = n,\ (a, b, d) = 1,\ 0 \leqslant b < d \right\}. \tag{1.2}$$

Thus $\boldsymbol{T} = \bigcup_{n=1}^{\infty} \boldsymbol{T}_n$, and the union is disjoint.

We have the following decomposition lemma.

LEMMA 1.1. *If $M \in M_2^+(\boldsymbol{Z})$, $n = \text{lev}(M)$, and $g = \gcd(M)$, then there are unique $M' \in \boldsymbol{T}_n$ and $S \in \Gamma(1)$ such that*

$$M = gSM'. \tag{1.3}$$

The set $\boldsymbol{T}_n$ is finite for each $n \in \boldsymbol{N}$ with cardinality

$$|\boldsymbol{T}_n| = \mu_0(n) = n \cdot \prod_{p|n} (1 + 1/p). \tag{1.4}$$

(This second equation is the definition of $\mu_0(n)$.)

LEMMA 1.2. *If $\text{lev}(M) = m$, $\gcd(M) = g$, then there are B, $S \in \Gamma(1)$ such that*

$$M = gS \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} B. \tag{1.5}$$

(See Schoeneberg [10], ch. VI, §3, for (1.3), (1.4) and (1.5).)

Lemma 1.1 allows us to make the following

DEFINITION 1.3. For any A, $M \in M_2^+(\boldsymbol{Z})$, we define $M^A \in \boldsymbol{T}$ by the equation

$$MA = gSM^A \tag{1.6}$$

for some $S \in \Gamma(1)$, and with $g = \gcd(MA)$.

For two integer matrices M, A, of any sizes such that AM is defined, we have

$$\gcd(A)\gcd(M) | \gcd(AM), \tag{1.7}$$

and if A is 2×2, and we let A^* be its adjoint, so that $A^*A = \det(A)I$ and $\gcd(A^*) = \gcd(A)$, then we have

(1.8) $$\gcd(A)\gcd(AM)\,|\,\det(A)\gcd(M).$$

In particular, if $\det(A) = 1$ then $\gcd(A) = 1$ and $\gcd(MA) = \gcd(AM) = \gcd(M)$ for every M. This implies, when $M \in M_2^+(\mathbf{Z})$, that

(1.9) $$\mathrm{lev}(MA) = \mathrm{lev}(AM) = \mathrm{lev}(M),$$

and we have the following:

LEMMA 1.4. *If $A \in \Gamma(1)$, then for each $n \in \mathbf{N}$*

(1.10) $$M \mapsto M^A$$

is a permutation of $\mathbf{T}_n$.

The matrices $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2^+(\mathbf{R})$ act on the upper half-plane $\mathbf{H} = \{\tau \in \mathbf{C} \mid \mathrm{Im}\,\tau > 0\}$ by linear fractional transformations:

$$M\tau = \frac{a\tau + b}{c\tau + d},$$

and we define the *automorphic factor* to be

$$(M:\tau) = c\tau + d.$$

For any $r \in \mathbf{R}$, any $f: \mathbf{H} \to \mathbf{C} \cup \{\infty\}$, and any $M \in M_2^+(\mathbf{R})$, we define the *stroke operator* of degree $-r$ (weight r) by

(1.11) $$f|M = (\det(M))^{+r/2}(M:\tau)^{-r} f(M\tau),$$

where the power is determined by the principal branch of the logarithm: $-\pi < \arg(z) \leqslant \pi$. It follows that for any $M, S \in M_2^+(\mathbf{R})$ there is a constant $\sigma(M, S)$ (dependent on r) of modulus 1 such that

(1.12) $$f|MS = \sigma(M, S)\cdot f|M|S.$$

Suppose $\Gamma \leqslant \Gamma(1)$ is a subgroup of finite index. Let $\frac{1}{0} = \infty$ be the point at infinity of $\mathbf{C}$, let $\mathbf{Q}^* = \mathbf{Q} \cup \{\infty\}$, and set $U^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. For any $\zeta \in \mathbf{Q}^*$ we choose any $A \in \Gamma(1)$ such that $A\zeta = \infty$ and define the *width* of Γ at ζ to be

(1.13) $$\kappa(\Gamma; \zeta) = \min\{n \in \mathbf{N} \mid \pm A^{-1} U^n A \in \Gamma\}.$$

DEFINITION 1.5. Suppose $\Gamma \leqslant \Gamma(1)$ is a subgroup of finite index, $r \in \mathbf{R}$, and $v: \Gamma \to \{\xi \in \mathbf{C} \mid |\xi| = 1\}$, and $\mathbf{C}^* = \mathbf{C} \cup \{\infty\}$ is the Riemann sphere. Then we say $f: \mathbf{H} \to \mathbf{C}^*$ is a *form of degree $-r$ on Γ with multiplier system v* provided

(i) f is meromorphic on $\mathbf{H}$,

(ii) $f|_{(-r)}V = v(V)\cdot f$ for all $V \in \Gamma$, and

(iii) for each $A \in \Gamma(1)$ there is some $\varkappa \in [0, 1)$, $m_0 \in \mathbf{Z}$, $b_m \in \mathbf{C}$, and $h \geqslant 0$ such that in the region $\mathrm{Im}(A\tau) > h$, we have a series representation

(1.14) $$f(\tau) = (A:\tau)^r \sum_{m=m_0}^{\infty} b_m e^{2\pi i(m+\varkappa)A\tau/N},$$

where $N = \kappa(\Gamma;\ A^{-1}(\infty))$.

By $\{\Gamma,\ -r,\ v\}$ we denote the set of all forms of degree $-r$ on Γ with multiplier system v, and we say simply that f is a *modular form* if $f \in \{\Gamma,\ -r,\ v\}$ for some r, some v, and some Γ of finite index in $\Gamma(1)$. If $f \in \{\Gamma,\ -r,\ v\}$ and $f \neq 0$, and if $\zeta = A^{-1}(\infty)$, then we can assume that $b_{m_0} \neq 0$ in (1.10), and then the *order of f with respect to Γ at ζ* is defined by

(1.15) $$\mathrm{Ord}_\Gamma(f; \zeta) = m_0 + \varkappa.$$

We then define the *invariant order of f at ζ* by

(1.16) $$\mathrm{ord}(f; \zeta) = \frac{1}{\kappa(\Gamma; \zeta)} \cdot \mathrm{Ord}_\Gamma(f; \zeta).$$

The invariant order is so-called because it does not depend on the choice of Γ. Working with the invariant order is sometimes useful because it satisfies the following transformation formula:

LEMMA 1.6. *Suppose $r, s \in \mathbf{Z}$, $(r, s) = 1$, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2^+(\mathbf{Z})$. Let $m = \det(M)$, and $g = \gcd(ar + bs,\ cr + ds)$. Then*

(1.17) $$\mathrm{ord}\left(f|M, \frac{r}{s}\right) = \frac{g^2}{m}\,\mathrm{ord}\left(f; M\frac{r}{s}\right).$$

(Cf. Berndt, Biagioli, and Purtilo [1].) Note that g is the factor that cancels when the fraction $M\frac{r}{s}$ is reduced to lowest terms.

If f is a modular form and $M \in M_2^+(\mathbf{Z})$ with $\mathrm{lev}(M) = n$, then $f|M$ is called the transform of f by M, and $f|M$ is said to be a transform of f of level n.

For two functions f and g, we use the notation

$$f = \sim g$$

to mean that $f = \gamma g$ for some non-zero constant γ. If f is a form on $\Gamma(1)$, then combining (1.3) and (1.12) and (ii) of the definition of modular forms, we see that for every $M \in M_2^+(\mathbf{Z})$ there is some $M' \in \mathbf{T}$ so that

$$f|M = \sim f|M',$$

and thus $\{f|M:\ M \in \mathbf{T}_n\}$, which is a finite set, is essentially all of the transforms of f of level n.

The Dedekind eta function is a form on the full modular group $\Gamma(1)$ of degree $-1/2$ (cf. Knopp [4], Rademacher [9], or any of many elementary texts treating modular forms), and, since $\kappa(\Gamma(1);\ \zeta) = 1$ for all $\zeta \in \mathbf{Q}^*$,

$$\mathrm{ord}(\eta; \zeta) = \mathrm{Ord}_{\Gamma(1)}(\eta; \zeta) = 1/24.$$

If $\mathrm{lev}(M) = n$, then $\eta|M$ is a form of degree $-1/2$ on the *transform subgroup*

$$\Gamma_M = \Gamma(1) \cap M^{-1}\Gamma(1)M.$$

If $M = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$, then we get the transform $\eta|M(\tau) = \sim \eta(n\tau)$, which we call the *principal transform of level n*, and the transform subgroup for this M

$$\Gamma_M = \Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \,\middle|\, c \equiv 0 \pmod{n} \right\}$$

is called the principal transform subgroup. The transform groups of level n contain the *principal congruence subgroup* of level n:

$$\Gamma_M \supseteq \Gamma(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \,\middle|\, a \equiv d \equiv \pm 1 \pmod{n} \text{ and } b \equiv c \equiv 0 \pmod{n} \right\}.$$

Lemmas 1.2 and 1.4 have the following consequences for the eta transforms:

1. For every $M \in M_2^+(\mathbf{Z})$ with $\mathrm{lev}(M) = m$, there is an $A \in \Gamma(1)$ such that

$$\eta|M|A = \sim \eta(m\tau). \tag{1.18}$$

2. For any $m \in \mathbf{N}$ and $A \in \Gamma(1)$ the transforms $\eta|M$ for $M \in \mathbf{T}_m$ are essentially permuted by the stroke operator:

$$\eta|M|A = \sim \eta|M^A. \tag{1.19}$$

We need the following result:

LEMMA 1.7. *A modular form f with no zeros or poles in $\mathbf{H}$ and with $\mathrm{ord}(f;\zeta) = 0$ for all $\zeta \in \mathbf{Q}^*$ is constant.*

This follows from Knopp, Lehner, and Newman [5].

PART I: MULTIPLICATIVE INDEPENDENCE RESULTS

2. Sufficiency of the condition for star-equivalence. We can prove the converse part of Theorem A immediately:

PROPOSITION 2.1. *Suppose $n \in \mathbf{N}$, $r, s, r', s' \in \mathbf{Z}$, $(r, s) = (r', s') = 1$, $\alpha \in \mathbf{Z}$ is relatively prime to n, and*

$$\begin{pmatrix} r' \\ s' \end{pmatrix} \equiv \alpha \begin{pmatrix} r \\ s \end{pmatrix} \pmod{n}.$$

Then

$$\frac{r}{s} *\sim \frac{r'}{s'} \pmod{n}.$$

Proof. Take $M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathbf{T}_n$. Then, by (1.17),

$$\mathrm{ord}\left(f|M, \frac{r}{s}\right) = \tfrac{1}{24}(g^2/n), \quad \text{where } g = \gcd\begin{pmatrix} ar+bs \\ ds \end{pmatrix},$$

$$\mathrm{ord}\left(f|M, \frac{r'}{s'}\right) = \tfrac{1}{24}(g'^2/n), \quad \text{where } g' = \gcd\begin{pmatrix} ar'+bs' \\ ds' \end{pmatrix},$$

so it is sufficient to show that $g = g'$. Since $g = \gcd\left(M\begin{pmatrix} r \\ s \end{pmatrix}\right)$, and this divides $\det(M)\gcd\begin{pmatrix} r \\ s \end{pmatrix} = n$, we see that $g|n$ and similarly $g'|n$. From this we get

$$g' = (g', n) = (ar'+bs', ds', n) = (a\alpha r + b\alpha s, d\alpha, n) = (ar+bs, ds, n) = (g, n) = g,$$

so the lemma is proven.

3. A particular eta product. A key construction in our proof is the following eta product.

LEMMA 3.1. *For each $n \in \mathbf{N}$ there are rational numbers $\beta(M)$ for each $M \in \mathbf{T}_n$ such that the function*

$$\Delta_n = \prod_{M \in \mathbf{T}_n} (\eta|M)^{\beta(M)} \tag{3.1}$$

satisfies

$$\mathrm{ord}\left(\Delta_n; \frac{r}{s}\right) = \begin{cases} 1, & \text{if } n|s, \\ 0, & \text{if } n \nmid s. \end{cases} \tag{3.2}$$

In this section we shall construct Δ_n as a product of principal transforms, specifically as the appropriate power of the function ${}_1H_n$ appearing in the following definition and proposition. Then in Section 4 we will conclude the proof of Lemma 3.1 by showing that Δ_n can also be written as a product of transforms by $M \in \mathbf{T}_n$, i.e. as a product of transforms of level exactly n.

DEFINITION 3.2. Suppose $a, d \in \mathbf{N}$ and μ is the Möbius μ-function. Then we define

$${}_dH_a(\tau) = \prod_{\delta|d} \prod_{\alpha|a} \eta(\delta\alpha\tau)^{\mu(\delta)\frac{d}{\delta}\mu(\frac{a}{\alpha})\alpha}.$$

PROPOSITION 3.3. *If $r, s \in \mathbf{Z}$ and $(r, s) = 1$, then*

$$\mathrm{ord}\left({}_dH_a; \frac{r}{s}\right) = \begin{cases} \frac{1}{24}a^2 d \prod_{p|ad}(1-1/p^2), & \text{if } (s, ad) = a, \\ 0, & \text{if } (s, ad) \neq a. \end{cases} \tag{3.3}$$

Specific examples of these functions have appeared previously in the literature, for instance, in W. H. H. Petersson [8], and in the recent investigations of the character tables of the Monster group, e.g. in Conway and Norton [2] (Table 3, pp. 332–334), but this presentation as a family seems to be new.

Proof. Let $M = \begin{pmatrix} \alpha\delta & 0 \\ 0 & 1 \end{pmatrix}$ where α and δ are divisors of a and d, respectively, and apply (1.13) to get

$$\operatorname{ord}\left(\eta(\alpha\delta\tau); \frac{r}{s}\right) = \tfrac{1}{24}(\alpha\delta, s)^2/(\alpha\delta),$$

and, summing over all α, δ, we have

$$\operatorname{ord}\left({}_dH_a; \frac{r}{s}\right) = \frac{d}{24}\psi(a, d),$$

where

$$\psi(a, d) = \sum_{\delta|d}\sum_{\alpha|a} \frac{(\alpha\delta, s)^2}{\delta^2}\mu(\delta)\mu\left(\frac{a}{\alpha}\right). \tag{3.4}$$

We can factor

$$\psi(a, d) = \prod_p \psi(p^c, p^\gamma),$$

where p^c and p^γ are the highest powers of the prime p dividing a and d, respectively, because the functions $\psi_1(a, d) = \dfrac{(ad, s)^2}{d^2}\mu(d)$ and $\psi_2(a, d) = \mu(a)$ have this factorization property, and the terms in the sum (3.4) are $\psi_1(\alpha, \delta)\cdot\psi_2\left(\dfrac{a}{\alpha}, \dfrac{d}{\delta}\right)$. (This is analogous to the property of multiplicative functions of one variable.) Thus we need only consider

$$\psi(p^c, p^\gamma) = \sum_{i=0}^{c}\sum_{j=0}^{\gamma} \frac{(p^{i+j}, s)^2}{p^{2j}}\mu(p^j)\mu(p^{c-i}). \tag{3.5}$$

Those terms with $i < c-1$, or $j > 1$ are zero, because of the factors $\mu(p^j)\mu(p^{c-i})$.

The case $c = \gamma = 0$ does not occur. Otherwise,

$$\psi(p^c, p^\gamma) = \begin{cases} \left(1 - \dfrac{(p, s)^2}{p^2}\right), & \text{if } c = 0, \\ (p^c, s)^2 - (p^{c-1}, s)^2, & \text{if } \gamma = 0, \\ (p^c, s)^2 - (p^{c-1}, s)^2 - (1/p^2)[(p^{c+1}, s)^2 - (p^c, s)^2], & \\ \qquad\qquad \text{if } c > 0, \text{ and } \gamma > 0. & \end{cases} \tag{3.6}$$

Now we see that $\psi(p^c, p^\gamma) = 0$ if either $p^c \nmid s$, or $p^{c+1} | s$, and that otherwise $\psi(p^c, p^\gamma) = p^{2c}(1 - 1/p^2)$.

Thus if $(ad, s) \neq a$ then one of the factors $\psi(p^c, p^\gamma)$ is 0, and so $\psi(a, d) = 0$, and when $(ad, s) = a$, we have $\psi(a, d) = a^2 \prod_{p|ad}(1 - 1/p^2)$.

This completes the proof of the proposition.

4. Uniformizing the level. To complete the proof of Lemma 3.1, we let

$$\alpha = \frac{1}{24}n^2\prod_{p|n}\left(1 - \frac{1}{p^2}\right), \tag{4.1}$$

and

$$\Delta_n = {}_1H_n^{1/\alpha}. \tag{4.2}$$

Then equation (3.2) follows from Proposition 3.3. What remains to be shown is (3.1), i.e., the existence of the exponents $\beta(M)$. This is a consequence of the following:

LEMMA 4.1. *Suppose $\alpha(M)$ is a real number for each $M \in M_2^+(\mathbf{Z})$, only a finite number of which are non-zero, and suppose that $\alpha(M) \neq 0$ only when $\operatorname{lev}(M)$ is a divisor of n. Let*

$$h(\tau) = \prod_M (\eta | M(\tau))^{\alpha(M)}.$$

Then there are real numbers $\beta(M)$ for $M \in \mathbf{T}_n$ which are rational linear combinations of the $\alpha(M)$ such that

$$h(\tau) = \sim \prod_{M \in \mathbf{T}_n} (\eta | M(\tau))^{\beta(M)}. \tag{4.3}$$

Remark. By (1.18) and (1.19) it is sufficient to prove the assertion in the case $h(\tau) = \eta(m\tau)$ for any $m|n$. (In fact, this is more precisely what we need to complete the proof of Lemma 3.1, but the more general statement is true, and an immediate consequence, so we make it.) Our proof will depend on the form of some multiplicative identities which we establish in Propositions 4.2 and 4.3.

PROPOSITION 4.2. *Let $\xi = e^{2\pi i/48}$, and let σ and μ be the divisor sum function and the Möbius μ-function, respectively. Then*

$$\prod_{b=0}^{d-1} \eta\left(\tau + \frac{b}{d}\right) = \xi^{d-1}\prod_{\delta|d} \eta(\delta d\tau)^{\mu(\delta)\sigma\left(\frac{d}{\delta}\right)}. \tag{4.4}$$

Proof. We separate the identity into two parts: the first corresponding to the factor of $x^{1/24}$ in the definition of the eta function, and the second corresponding to the product $\prod(1 - x^n)$. Thus, setting $e(\tau) = e^{2\pi i\tau/24}$, $q = e^{2\pi i\tau}$, and $\Phi(\tau) = \prod_{n=1}^{\infty}(1 - q^n)$, we have $\eta(\tau) = e(\tau)\Phi(\tau)$ and it is sufficient to show that

$$\prod_{b=0}^{d-1} e\left(\tau + \frac{b}{d}\right) = e\left(\frac{d-1}{2}\right)\prod_{\delta|d} e(\delta d\tau)^{\mu(\delta)\sigma(d/\delta)}, \tag{4.5}$$

and

$$\prod_{b=0}^{d-1} \Phi\left(\tau + \frac{b}{d}\right) = \prod_{\delta|d} \Phi(\delta d\tau)^{\mu(\delta)\sigma(d/\delta)}. \tag{4.6}$$

The first of these follows from $\sum_{b=0}^{d-1} b = d(d-1)/2$ and from

$$\sum_{\delta|d} \delta\mu(\delta)\sigma\left(\frac{d}{\delta}\right) = \prod_{p^\alpha \| d} \left(\sigma(p^\alpha) - p\sigma(p^{\alpha-1})\right) = 1. \tag{4.7}$$

The second requires some manipulation. First we note that if ξ is a primitive sth root of unity, t is any natural number, and $d = st$, then

$$\prod_{b=0}^{d-1} (1-\xi^b X) = (1-X^s)^t. \tag{4.8}$$

Setting $\varrho = e^{2\pi i/d}$, and letting P denote the left-hand side of (4.6), we have

$$P = \prod_{b=0}^{d-1} \Phi\left(\tau + \frac{b}{d}\right) = \prod_{n=1}^{\infty} \prod_{b=0}^{d-1} (1-\varrho^{nb}q^n). \tag{4.9}$$

If we set $t = (n, d)$ and $s = d/t$, then $\xi = \varrho^n$ is a primitive sth root of unity, and we get

$$P = \prod_{n=1}^{\infty} (1-q^{ns})^t. \tag{4.10}$$

(Keep in mind that s and t are functions of n and d.) We now decompose n modulo d as $n = md - c$ with $0 \leqslant c < d$. Then $t = (c, d)$ is independent of m, so

$$\begin{aligned} P &= \prod_{c=0}^{d-1} \left(\prod_{m=1}^{\infty} (1-q^{(md-c)s})\right)^t = \prod_{st=d} \prod_{\substack{d=0 \\ (c,d)=t}}^{d-1} \left(\prod_{m=1}^{\infty} (1-q^{(md-c)s})\right)^t \\ &= \prod_{st=d} \prod_{\substack{e=0 \\ (e,s)=1}}^{s-1} \left(\prod_{m=1}^{\infty} (1-q^{d(ms-e)})\right)^t = \prod_{st=d} \left(\prod_{\substack{n=1 \\ (n,s)=1}}^{\infty} (1-q^{dn})\right)^t. \end{aligned} \tag{4.11}$$

We apply a Möbius inversion in the form

$$\sum_{\substack{r|s \\ r|n}} \mu(r) = \begin{cases} 1, & \text{if } (n, s) = 1, \\ 0, & \text{if } (n, s) > 1. \end{cases}$$

Thus

$$\prod_{\substack{n=1 \\ (n,s)=1}}^{\infty} (1-q^{dn}) = \prod_{n=1}^{\infty} \prod_{\substack{r|n \\ r|s}} (1-q^{dn})^{\mu(r)} = \prod_{r|s} \left(\prod_{\substack{n=1 \\ r|n}}^{\infty} (1-q^{dn})\right)^{\mu(r)} \tag{4.12}$$

$$= \prod_{r|s} \left(\prod_{m=1}^{\infty} (1-q^{drm})\right)^{\mu(r)} = \prod_{r|s} \Phi(rd\tau)^{\mu(r)}.$$

Substituting this expression into (4.11), we have

$$P = \prod_{st=d} \prod_{r|s} \Phi(rd\tau)^{\mu(r)} = \prod_{r|d} \Phi(rd\tau)^{\mu(r)\sigma(d/r)}, \tag{4.13}$$

which is (4.6), and so the proof is complete.

To get an identity in which an arbitrary transform $\eta\left(\frac{a\tau+b}{d}\right)$ appears, we can substitute $\tau \mapsto a\tau/d$ in (4.4). When we do this, however, the transforms appearing on the left are not necessarily all reduced. For values of b such that $(a, b, d) = g \neq 1$, they will not be. Consequently, the levels, ad/g^2 of these terms are not all the same. To get an identity in which the left-hand side involves only transforms of the same level, ad, we do another Möbius inversion.

PROPOSITION 4.3. *With ξ, σ, and μ as in Proposition 4.2, with φ being the Euler totient function, and*

$$E(a, d) = \begin{cases} 1, & \text{if } (a, d) = 1, \\ 0, & \text{if } (a, d) > 1, \end{cases}$$

we have

$$\xi^{E(a,d)} \prod_{\substack{b=0 \\ (a,b,d)=1}}^{d-1} \eta\left(\frac{a\tau+b}{c}\right) = \xi^{d\frac{\varphi((a,d))}{(a,d)}} \prod_{\substack{t|a \\ rt|d}} \eta\left(\frac{ar}{t}\tau\right)^{\mu(r)\mu(t)\sigma(d/rt)} \tag{4.14}$$

Remark. Some specific examples of these identities appear in Conway and Norton [2], p. 333.

Proof. Applying Proposition 4.2,

$$\begin{aligned} \prod_{\substack{b=0 \\ (a,b,d)=1}}^{d-1} \eta\left(\frac{a\tau+b}{d}\right) &= \prod_{t|(a,d)} \prod_{c=0}^{d/t-1} \eta\left(\frac{a\tau+ct}{d}\right)^{\mu(t)} \\ &= \prod_{t|(a,d)} \left(\prod_{c=0}^{d/t-1} \eta\left(\frac{a/t+c}{d/t}\right)^{\mu(t)}\right. \\ &= \prod_{t|(a,d)} \left(\xi^{d/t-1} \prod_{r|d/t} \eta\left(r\frac{a}{t}\tau\right)^{\sigma(d/rt)\mu(r)}\right)^{\mu(t)} \\ &= \left(\prod_{t|(a,d)} \xi^{(d/t-1)\mu(t)}\right) \prod_{t|(a,d)} \prod_{rt|d} \eta\left(\frac{ar}{t}\tau\right)^{\sigma(d/rt)\mu(r)\mu(t)} \\ &= \xi^{\left(\frac{d}{(a,d)}\varphi((a,d)) - E(a,d)\right)} \prod_{\substack{t|a \\ rt|d}} \eta\left(\frac{ar}{t}\tau\right)^{\sigma(d/rt)\mu(r)\mu(t)} \end{aligned} \tag{4.15}$$

Proof of Lemma 4.1. For any natural numbers a and d we set

$$H[a, d](\tau) = \prod_{\substack{b=0 \\ (a,b,d)=1}}^{d-1} \eta\left(\frac{a\tau+b}{d}\right). \tag{4.16}$$

Then for a fixed n and any $ad = n$, (4.14) can be expressed as

$$H[a, d](\tau) = \sim \prod_{m|n} \eta(m\tau)^{\alpha(m)}, \tag{4.17}$$

for some rational numbers $\alpha(m)$. As a runs over the divisors of n this is a system of $\sigma_0(n)$ equations in the $\sigma_0(n)$ quantities $\eta(m\tau)$, where $\sigma_0(n)$ is the number of divisors of n. To prove Lemma 4.1 we will show that for each $m|n$ there are rational numbers $\beta(a)$ such that

$$\eta(m\tau) = \sim \prod_{ad=n} H[a, d]^{\beta(a)}. \tag{4.18}$$

Since $H[1, 1](\tau) = \eta(\tau)$, it seems plausible that we can proceed by considering one prime $p|n$, and reducing to an expression involving $H[a_0, d_0](\tau)$, where $p \nmid a_0$, and $p \nmid d_0$.

Suppose that a, d are natural numbers and that p is a prime which divides ad. Let $a = a_0 p^i$, and $d = d_0 p^j$, where $p \nmid a_0 d_0$. By (4.14), we have

$$H[a, d](\tau) = \sim \prod_{t|a,rt|d} \eta\left(\frac{ar}{t}\tau\right)^{\mu(r)\mu(t)\sigma(d/rt)}. \tag{4.19}$$

We separate the factors in this product according to the powers of p which divide each of r and t: $p^\varepsilon \| r$ and $p^\delta \| t$, where $0 \leqslant \varepsilon \leqslant j$ and $0 \leqslant \delta \leqslant \max(i, j-\varepsilon)$. We denote the resulting expression by $P_{\varepsilon,\delta}$ and we have

$$P_{\varepsilon,\delta} = \prod_{\substack{rt|d, t|a \\ p^\varepsilon \| r, p^\delta \| t}} \eta\left(\frac{ar}{t}\tau\right)^{\mu(r)\mu(t)\sigma(d/rt)}. \tag{4.20}$$

When $\varepsilon > 1$ or $\delta > 1$, the exponent is zero, so $P_{\varepsilon,\delta} = 1$. If $j = 0$, or $\varepsilon > j$, or $i = 0$, we define any expressions $P_{\varepsilon,\delta}$ for which the corresponding product is empty to be $P_{\varepsilon,\delta} = 1$. Then we have

$$H[a, d] = P_{0,0} P_{0,1} P_{1,0} P_{1,1}. \tag{4.21}$$

We define r_0 and s_0 by $r = p^\varepsilon r_0$ and $s = p^\delta s_0$. Then as r runs over the divisors of a, r_0 runs over the factors of a_0, and similarly for s_0 and d_0. In addition, the exponent $\mu(r)\mu(s)\sigma(d/rt)$ is multiplicative, so we have

$$P_{\varepsilon,\delta} = H[a_0, d_0](p^{i+\varepsilon-\delta}\tau)\mu(p^\varepsilon)\mu(p^\delta)\sigma(p^{j-\alpha-\delta}). \tag{4.22}$$

To write this more compactly, we set $F_l(\tau) = h[a_0, d_0](p^l\tau)$, and $\sigma[l] = \sigma(p^l) = p^l + \ldots + p + 1$, for any $l \geqslant 0$. Thus (4.22) becomes

$$\begin{aligned} P_{0,0} &= F_i^{\sigma[j]}, & P_{1,0} &= F_{i+1}^{-\sigma[j-1]}, \\ P_{0,1} &= F_{i-1}^{-\sigma[j-1]}, & P_{1,1} &= F_i^{\sigma[j-2]}, \end{aligned} \tag{4.23}$$

whenever the F_l and $\sigma[l]$ are defined. To cover all cases, we set $F_{-1} = 1$, and $\sigma[-1] = \sigma[-2] = 0$. Looking again at (4.21), we have

$$H[a, d] = \sim \frac{F_i^{\sigma[j]} F_i^{\sigma[j-2]}}{F_{i-1}^{\sigma[j-1]} F_{i+1}^{\sigma[j-1]}}. \tag{4.24}$$

If we set $\alpha = i+j$, and $G_{\alpha,k} = \dfrac{F_k^{\sigma[\alpha-k]}}{F_{k+1}^{\sigma[\alpha-k-1]}}$, then (4.24) becomes

$$H[a_0 p^i, d_0 p^j] = \sim \frac{G_{\alpha,i-1}}{G_{\alpha,i}}.$$

Then

$$\prod_{i=k+1}^{\alpha} H[a_0 p^i, d_0 p^j] = \sim \frac{G_{\alpha,k}}{G_{\alpha,\alpha}} = G_{\alpha,k}.$$

(Here we use $G_{\alpha,-1} = F_0^{\sigma[\alpha]}$ and $G_{\alpha,\alpha-1} = F_\alpha$.) By the definition of $G_{\alpha,k}$, we have

$$F_{k+1}^{\sigma[\alpha-k-1]} = \sim F_k^{\sigma[\alpha-k-2]} \prod_{i=k+1}^{\alpha} H[a_0 p^i, d_0 p^j].$$

We fix a numer α and then by induction on k it follows that there are rational numbers $\beta_{i,k}$ such that

$$H[a_0, d_0](p^k\tau) = F_k = \prod_{i+j=\alpha} (H[a_0 p^i, d_0 p^j])^{\beta_{i,k}}.$$

By induction on the number of primes dividing m, we see that there are rational numbers $\beta(a)$ such that

$$H[a_0, d_0](m\tau) = \sim \prod_{ad=n} H[a, d](\tau)^{\beta(a)}$$

whenever $a_0 d_0 \| n$, and $a_0 d_0 m | n$. (In fact, we can assert that $\beta(a) \neq 0$ only when $a_0 \| a$.) Taking $a_0 = d_0 = 1$, we have the Lemma 4.1, since each $H[a, d]$ is a product of transforms of level exactly $ad = n$.

5. Proofs of Theorems A, B, C, and D.

LEMMA 5.1. *Suppose* $n \in N$, $\zeta, \zeta' \in \boldsymbol{Q}^*$, *and* $A \in \Gamma(1)$. *Then* $\zeta * \sim \zeta' \pmod n$ *if and only if* $A\zeta * \sim A\zeta' \pmod n$.

Proof. If $\mathrm{lev}(M) = n$, then $\mathrm{lev}(MA) = n$, so

$$\mathrm{ord}(\eta|M; A\zeta) = \mathrm{ord}(\eta|MA; \zeta) = \mathrm{ord}(\eta|MA; \zeta') = \mathrm{ord}(\eta|M; A\zeta').$$

Proof of Theorem A. The converse part of the theorem was proven in §2. For the direct part, let us suppose $r, s, r', s' \in \boldsymbol{Z}$, $(r, s) = (r', s') = 1$, and

$\frac{r}{s} * \sim \frac{r'}{s'} \pmod n$, i.e.,

$$\text{ord}\left(\eta|M; \frac{r}{s}\right) = \text{ord}\left(\eta|M; \frac{r'}{s'}\right) \quad \text{whenever } \text{lev}(M) = n. \tag{5.1}$$

Choose $A \in \Gamma(1)$ so that $A\frac{r}{s} = \frac{1}{0}$ and set $\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = A\begin{pmatrix}r'\\ s'\end{pmatrix}$, so that $\frac{1}{0} * \sim \frac{\alpha}{\beta} \pmod n$. Since Δ_n is a product of transforms of level n (Lemma 4.1),

$$\text{ord}\left(\Delta_n; \frac{1}{0}\right) = \text{ord}\left(\Delta_n; \frac{\alpha}{\beta}\right).$$

By the definition of Δ_n (see (3.2)), this implies that $\beta \equiv 0 \pmod n$. Thus

$$A\begin{pmatrix}r'\\ s'\end{pmatrix} = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \equiv \alpha\begin{pmatrix}1\\ 0\end{pmatrix} \pmod n.$$

Applying A^{-1} to this congruence yields $\begin{pmatrix}r'\\ s'\end{pmatrix} \equiv \alpha\begin{pmatrix}r\\ s\end{pmatrix} \pmod n$, and this completes the proof of Theorem A.

LEMMA 5.2. *The number of equivalence classes under star-equivalence modulo n is*

$$\mu_0(n) = n\prod_{p|n}(1+1/p). \tag{5.2}$$

Proof. Consider $\mathscr{S} = \{(r, s)\colon 0 \leqslant r, s < n \text{ and } (r, s, n) = 1\}$. Then

$$|\mathscr{S}| = n^2\prod_{p|n}(1-1/p^2) = \mu_0(n)\varphi(n).$$

(See Schoeneberg [10], ch. IV, § 2.) Let ψ: $\boldsymbol{Q}^* \to \mathscr{S}$ be defined by $\psi(r/s) = (r', s')$ where $(r, s) = 1$, $r' \equiv r \pmod n$, and $s' \equiv s \pmod n$. ψ is onto. (See Schoeneberg [10].) For $\zeta \in \boldsymbol{Q}^*$, we let $[\zeta]$ be the equivalence class of ζ under star-equivalence modulo n. By Theorem A, $\phi([\zeta])$ has $\phi(n)$ elements for each ζ. Consequently there are $\mu_0(n)$ equivalence classes.

Proof of Theorem B. By Theorem A, the number k of equivalence classes under star-equivalence is finite, so we let $\zeta_1, \ldots, \zeta_k$ be cusps chosen one from each equivalence class. Choose $A_i \in \Gamma(1)$ so that $A_i\zeta_i = \infty$ and set $\delta_i = \Delta_n|A_i$ (the $|$ is the stroke operator). Then for any $\zeta \in \boldsymbol{Q}^*$, we have

$$\text{ord}(\delta_i; \zeta) = \begin{cases}1, & \text{if } \zeta * \sim \zeta_i \pmod n,\\ 0, & \text{if not.}\end{cases}$$

Let $\beta_{M,i} = \text{ord}(\eta|M; \zeta_i)$ and consider the function $(\eta|M)/\prod_{i=1}^{k}\delta_i^{\beta_{M,i}}$. This function has order zero at every cusp, and has no zeros or poles in $\boldsymbol{H}$ so it is constant. Thus

$$\eta|M = \sim \prod_{i=1}^{k}\delta_i^{\beta_{M,i}}. \tag{5.3}$$

There are rational numbers $\alpha_{i,M}$ (cf. Lemmas 1.1, 1.4, and 3.1) such that

$$\delta_i = \sim \prod_{M \in \boldsymbol{T}_n}(\eta|M)^{\alpha_{i,M}}. \tag{5.4}$$

Substituting (5.3) into (5.4) yields

$$\delta_i = \sim \prod_{j=1}^{k}\delta_j^{\sum_M \beta_{M,j}\alpha_{i,M}},$$

and applying $\text{ord}(\,;\zeta_j)$ to both sides of this equation gives us

$$\sum_M \alpha_{i,M}\beta_{M,j} = \begin{cases}1, & \text{if } i = j,\\ 0, & \text{if } i \neq j.\end{cases} \tag{5.5}$$

Since, by the lemma and (1.4), the matrix $(\alpha_{i,M})$ is square, it is invertible.

Now suppose c_M are any real numbers such that

$$\prod_{M \in \boldsymbol{T}_n}(\eta|M)^{c_M} = \sim 1, \tag{5.6}$$

i.e., the function is constant. Then substituting (5.3) into (5.6), and evaluating the order at ζ_i, we see that $\sum_M \alpha_{i,M}c_M = 0$ for all i, and hence that $c_M = 0$ for each M. This completes the proof of Theorem B.

Proof of Theorem C. Suppose f is a modular form with no zeros or poles in $\boldsymbol{H}$ such that $\text{ord}(f;\zeta) = \text{ord}(f;\zeta')$ whenever $\zeta * \sim \zeta' \pmod n$. Take $\zeta_1, \ldots, \zeta_k$, and $\delta_1, \ldots, \delta_k$ as in the proof of Theorem B. Set

$$g = \prod_{i=1}^{k}\delta_i^{\text{ord}(f;\zeta_i)}.$$

Then $\text{ord}(f/g;\zeta) = 0$ for all $\zeta \in \boldsymbol{Q}^*$.

Let $\Gamma \leqslant \Gamma(1)$ be a subgroup with $(\Gamma(1):\Gamma) < \infty$ such that f is a form on Γ and set $\Gamma' = \Gamma \cap \Gamma(n)$. Under the homomorphism $\Gamma \to \Gamma(1)/\Gamma(n)$, the kernel is Γ', and $\Gamma/\Gamma' \simeq \text{image}(\Gamma)$ is finite. Hence $(\Gamma(1):\Gamma') < \infty$.

Since both f and g are forms on Γ', Lemma 1.7 implies $f/g = \sim 1$, or $f = \sim g$, so f is an eta product.

Conversely, if $f = \sim \prod_M(\eta|M)^{c_M}$, then f has no zeros or poles in $\boldsymbol{H}$, and setting n to be the least common multiple of the levels of those M for which $d_M \neq 0$, we see, by Lemma 4.1, we can find numbers c'_M for $M \in \boldsymbol{T}_n$ so that

$$f = \sim \prod_{M \in \boldsymbol{T}_n}(\eta|M)^{c'_M},$$

and then $\text{ord}(f;\zeta) = \text{ord}(f;\zeta')$ by the definition of star-equivalence, so Theorem C is proven.

Proof of Theorem D. The uniqueness follows from Theorem B, so suppose h is an eta product which is a form on $\Gamma(n)$. By Lemma 4.1 and the

definition of star-equivalence, there is some natural number m such that

$$\zeta *\sim \zeta' (\mathrm{mod}\, m) \Rightarrow \mathrm{ord}(h;\zeta) = \mathrm{ord}(h;\zeta'). \tag{5.7}$$

Suppose we can show that this holds with m replaced by n (note that, in general, $m \neq n$). Then we can take ζ_i and δ_i as in the proof of Theorem B, set $\beta_i = \mathrm{ord}(h;\zeta_i)$, and we then have

$$h = \sim \prod \delta_i^{\beta_i},$$

because the orders agree everywhere. This will complete the proof of Theorem D because of (5.4).

So suppose $\zeta *\sim \zeta' \pmod m$, and take $r, s, r', s' \in \boldsymbol{Z}$ so that $\zeta = r/s$, $\zeta' = r'/s'$, and $(r, s) = (r', s') = 1$. By Theorem A, there is some α, relatively prime to n, such that $\begin{pmatrix} r' \\ s' \end{pmatrix} \equiv \alpha \begin{pmatrix} r \\ s \end{pmatrix}$. Choose α_1 so that $\alpha_1 \equiv \alpha \pmod n$ and so that α_1 is relatively prime to m. Then $(\alpha_1 r, \alpha_1 s, [m, n]) = 1$, so we can find r'' so that $r'' \equiv \alpha_1 r \pmod{[m, n]}$ and $(r'', \alpha_1 s) = 1$. Setting $s'' = \alpha_1 s$ and $\zeta'' = r''/s''$, another application of Theorem A yields $\zeta'' *\sim \zeta \pmod m$, so that $\mathrm{ord}(h;\zeta'') = \mathrm{ord}(h;\zeta)$. Modulo n, we have

$$\begin{pmatrix} r'' \\ s'' \end{pmatrix} \equiv \alpha \begin{pmatrix} r \\ s \end{pmatrix} \equiv \begin{pmatrix} r' \\ s' \end{pmatrix},$$

so ζ'' and ζ are equivalent cusps modulo $\Gamma(n)$ (see Schoeneberg [10], p. 86), and thus $\mathrm{ord}(h;\zeta'') = \mathrm{ord}(h;\zeta')$. Hence we have shown that $\zeta *\sim \zeta' \pmod n$ implies $\mathrm{ord}(h;\zeta) = \mathrm{ord}(h;\zeta')$, and this completes the proof of Theorem D.

PART II: MULTIPLICATIVE BASES FOR THE FAMILY OF ETA PRODUCTS ON A SPECIFIC SUBGROUP OF $\Gamma(1)$

In Part I we established some results concerning multiplicative relationships between eta products. We now wish to determine multiplicative bases for the family of eta products which are modular forms on a given subgroup $\Gamma \leqslant \Gamma(1)$ of finite index. We shall give only a very brief description of a basis in the general case in § 6, and in §§ 7-9 shall give a detailed description of a more practical multiplicative basis for the principal transform subgroups $\Gamma_0(n)$.

6. Forms on $\Gamma(n)$ and arbitrary subgroups. We let

$$\mathscr{E} = \{\textstyle\prod \eta|M^{\alpha(M)}\colon\ M \in M_2^+(\boldsymbol{Z}),\ \text{only finitely many } \alpha(M) \neq 0\}$$

be the set of all eta products, and for any Γ we let $\mathscr{G} = \mathscr{G}_\Gamma$ be the subset of $\mathscr{E}$ consisting of those eta products which are forms on Γ.

When the subgroup is the principal congruence subgroup $\Gamma = \Gamma(n)$, Theorem D of Part I showed that $\mathscr{H} = \{\eta|M\colon\ M \in \boldsymbol{T}_n\}$ is a multiplicative basis for $\mathscr{G}$.

Recall that the mapping $M \mapsto M^A$ is a permutation of $\boldsymbol{T}_n$, the set of primitive, reduced transformations of level n, for any $A \in \Gamma(1)$, and that this gives an action of Γ on $\boldsymbol{T}$ when A is restricted to matrices in $\Gamma(1)$, for any subgroup of $\Gamma(1)$. (Cf. Definition 1.3 and Lemma 1.4.) If $M \in \boldsymbol{T}_n$, then the orbit of M under this action lies entirely in $\boldsymbol{T}_n$. The following theorem describes a multiplicatively spanning set for the family $\mathscr{G}$ of eta products which are forms on Γ when Γ is a congruence subgroup, i.e., when $\Gamma(1) \geqslant \Gamma \geqslant \Gamma(n)$ for some $n \in \boldsymbol{Z}$.

PROPOSITION 6.1. *Suppose $\Gamma \leqslant \Gamma(1)$ is a subgroup of finite index and h is an eta product. Then h is a form on Γ if and only if it has a representation*

$$h = \gamma \cdot \prod_{M \in \boldsymbol{T}} (\eta|M)^{\alpha(M)} \tag{6.1}$$

where γ is a constant and $\alpha(M)$ are real numbers, only a finite number of which are non-zero, and which satisfy

$$\alpha(M^A) = \alpha(M) \tag{6.2}$$

for each $A \in \Gamma$.

Proof. We may assume that $\alpha(M) \neq 0$ only for $M \in \boldsymbol{T}_n$, for some $n \geqslant 1$. (Take n to be the least common multiple of the levels of those M in the original product for which $\alpha(M) \neq 0$, then apply Lemma 4.1.) Then, for any $A \in \Gamma$, we have $h|A^{-1} = \sim h$, (the constant is $v(A^{-1})$, cf. Definition 1.5 of modular forms) and also

$$h|A^{-1} = \sim \prod_{M \in \boldsymbol{T}_n} (\eta|MA^{-1})^{\alpha(M)} = \sim \prod_{M \in \boldsymbol{T}_n} (\eta|M^{A^{-1}})^{\alpha(M)} = \sim \prod_{M \in \boldsymbol{T}_n} (\eta|M)^{\alpha(M^A)},$$

so

$$\prod_{M \in \boldsymbol{T}_n} (\eta|M)^{\alpha(M)} = \sim \prod_{M \in \boldsymbol{T}_n} (\eta|M)^{\alpha(M^A)},$$

and the theorem follows from Theorem B of Part I.

Now we can give a multiplicative basis for $\mathscr{G}$.

THEOREM 6.2. *Suppose $\Gamma(1) \geqslant \Gamma \geqslant \Gamma(n)$, suppose $M \in \boldsymbol{T}$, let $\langle M \rangle = \{M^A |\ A \in \Gamma\}$ be the orbit of M under the action of Γ, and define*

$$\eta|\langle M \rangle = \prod_{N \in \langle M \rangle} \eta|N.$$

Then a multiplicative basis for the family $\mathscr{G}$ of eta products which are forms on Γ is

$$\mathscr{H} = \{\eta|\langle M \rangle\colon\ M \in \boldsymbol{T}_n\}.$$

It is perhaps expected, but noteworthy nonetheless, that we do not obtain new forms on Γ by using eta products of levels higher than the conductor n of Γ (the least n such that $\Gamma \geqslant \Gamma(n)$).

Proof. Suppose h is an eta product and a form on Γ. Since $\Gamma \geqslant \Gamma(n)$, Theorem D shows that h can be written in the form

$$h = \prod_{M \in \boldsymbol{T}_n} (\eta|M)^{\alpha(M)},$$

and then the proof of Proposition 6.1 shows that h is in the multiplicative span of $\mathscr{H}$. From Theorem D again, it follows that $\mathscr{H}$ is multiplicatively independent.

7. The basis of level n for $\Gamma_0(n)$. In this section we describe more precisely the multiplicative basis for $\mathscr{G}$ given by Theorem 6.2 when the subgroup is $\Gamma = \Gamma_0(n)$. This basis turns out not to be very natural because it does not contain the principal transforms $\eta(a\tau)$, $a|n$. A multiplicative basis which is constructed around these transforms, and which, when it does contain other eta products, contains only eta products which involve the least number of factors possible, is constructed in §§8 and 9. Section 8 will produce a multiplicatively spanning set which contains the principal transforms and which is fairly close to a basis, having a few extra members in general, and Section 9 will give the final reduction to a multiplicatively independent set.

We now describe the orbit $\langle M \rangle$ of an arbitrary $M \in \boldsymbol{T}$ under the action of $\Gamma_0(n)$. If b and c are relatively prime to n, we say that b and c are in the same *quadratic class* modulo n, and we write

$$b \sim c \pmod{n}, \tag{7.1}$$

provided there is some integer δ, relatively prime to n, such that

$$b \equiv c\delta^2 \pmod{n}.$$

It is equivalent to say there is some δ such that $bc \equiv \delta^2 \pmod{n}$, i.e., bc is a quadratic residue modulo n.

PROPOSITION 7.1. *Suppose n is a natural number, and*

$$M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \quad \text{and} \quad M' = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$$

are in $\boldsymbol{T}$ with $ad|n$ and $a'd'|n$. Then M and M' are in the same orbit under the action of $\Gamma_0(n)$, i.e., there exists $A \in \Gamma_0(n)$ such that $M' = M^A$, if and only if

$$\begin{aligned} a' &= a, \\ d' &= d, \\ b' &\sim b \pmod{(a, d)}. \end{aligned} \tag{7.2}$$

Proof. Suppose $A = \begin{pmatrix} \alpha & \beta \\ \gamma n & \delta \end{pmatrix} \in \Gamma_0(n)$ and consider

$$MA = \begin{pmatrix} a\alpha + b\gamma n & a\beta + b\delta \\ d\gamma n & d\delta \end{pmatrix}.$$

The greatest common divisor of the first column, since $ad|n$, is a, so there is some $S \in \Gamma(1)$ and b' with $0 \leqslant b' < d$ so that

$$MA = S\begin{pmatrix} a & b' \\ 0 & d \end{pmatrix}.$$

We set $D = n/a$. Then $d|D$ and

$$S = \begin{pmatrix} \alpha + b\gamma D & * \\ d\gamma D & * \end{pmatrix}.$$

Modulo (a, d), we then have

$$MA \equiv \begin{pmatrix} 0 & b\delta \\ 0 & 0 \end{pmatrix} \equiv \begin{pmatrix} \alpha & * \\ 0 & * \end{pmatrix}\begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 & \alpha b' \\ 0 & 0 \end{pmatrix}.$$

Since $\alpha\delta \equiv 1 \pmod{n}$, this gives us $b' \equiv b\delta^2 \pmod{(a, d)}$, so that $b' \sim b \pmod{(a, d)}$.

Now suppose $ad|n$ and $b \sim b' \pmod{(a, d)}$. Choose δ so that $b' \equiv b\delta^2 \pmod{(a, d)}$ and so that $(\delta, n) = 1$. We can then find α, β, and γ so that $A = \begin{pmatrix} \alpha & \beta \\ \gamma n & \delta \end{pmatrix} \in \Gamma_0(n)$. By the first part of the proof, there are $S \in \Gamma(1)$ and b'' in $0 \leqslant b'' < d$ so that

$$MA = S\begin{pmatrix} a & b'' \\ 0 & d \end{pmatrix}$$

and this b'' satisfies $b'' \equiv b\delta^2 \equiv b' \pmod{(a, d)}$. Choosing k, l so that $b'' = b' + ak + dl$, we have

$$M(AU^{-k}) = (SU^l)\begin{pmatrix} a & b' \\ 0 & d \end{pmatrix}.$$

Since $AU^{-k} \in \Gamma_0(n)$, this completes the proof.

8. Reducing the level of the spanning set. Suppose $ad|n$, and $M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \boldsymbol{T}$. Then, following Proposition 7.1 and Theorem 6.2 we define

$$\langle M \rangle = \prod_{c \in C} \eta|\begin{pmatrix} a & c \\ 0 & d \end{pmatrix} \tag{8.1}$$

where

$$C = \{c \in \boldsymbol{Z} \mid 0 \leqslant c < d \text{ and } c \sim b \pmod{(a, d)}\}.$$

(This was denoted by $\eta|\langle M \rangle$ in Theorem 6.2.) Then $\langle M \rangle$ is a form on $\Gamma_0(ad)$, and consequently also a form on $\Gamma_0(n)$.

We let

$$\mathscr{H}_0 = \{\langle M \rangle \mid M \in \boldsymbol{T}_n\},$$

and

$$\mathscr{H} = \{\langle M\rangle |\ M \in \mathbf{T}_m \text{ for some } m|n\}.$$

By Proposition 7.1, $\mathscr{H}_0$ is a multiplicative basis for the family $\mathscr{G}$, and $\mathscr{H} \supseteq \mathscr{H}_0$, so $\mathscr{H}$ is a multiplicatively spanning set for $\mathscr{G}$ which contains the principal transforms. In this and the next section we reduce $\mathscr{H}$, first to a set $\mathscr{H}'$ and then to a set $\mathscr{H}''$, each of which is still a multiplicatively spanning set for $\mathscr{G}$, and then show that $\mathscr{H}''$ is a multiplicative basis for $\mathscr{G}$.

Before describing $\mathscr{H}'$ and $\mathscr{H}''$, we consider the properties of the relation $b \sim c \pmod m$ introduced above. Let $[b]_m = \{c \in \mathbf{Z} |\ b \sim c \pmod m\}$ be the quadratic class of b modulo m whenever $(b, m) = 1$. If k is the number of incongruent solutions modulo m of the equation $x^2 \equiv 1 \pmod m$, then $[b]_m$ contains $\varphi(m)/k$ incongruent elements, and this means there are k quadratic classes modulo m. If p is an odd prime, then $x^2 \equiv 1 \pmod{p^\alpha}$ has two solutions, and if $\alpha \geqslant 2$, then $x^2 \equiv 1 \pmod{2^\alpha}$ has the solutions $x \equiv \pm 1 \pmod{2^{\alpha-1}}$. Hence, if we let $\omega_1(m)$ denote the number of quadratic classes modulo m, we have

$$\omega_1(m) = \omega_1(2^\alpha)2^r,$$

where r is the number of odd primes dividing m, $2^\alpha \| m$, and

$$\omega_1(2^\alpha) = \begin{cases} 1, & \text{if } \alpha = 0, 1, \\ 2, & \text{if } \alpha = 2, \\ 4, & \text{if } \alpha \geqslant 3. \end{cases}$$

If $d|m$, then $b \sim c \pmod m$ implies $b \sim c \pmod d$. Thus there is a map $[b]_m \mapsto [b]_d$, which is a surjection, and this is a bijection if and only if $\omega_1(m) = \omega_1(d)$. There is a least divisor of m which has the same number of quadratic classes as m and its value we call the *quadratic radical of m*, and denote it by

$$\operatorname{qrad}(m) = 2^\beta \prod_{\substack{p|m \\ p \text{ odd}}} p,$$

where

$$\beta = \begin{cases} 0, & \text{if } 4 \nmid m, \\ 2, & \text{if } 4|m,\ 8 \nmid m, \\ 3, & \text{if } 8|m. \end{cases}$$

Note that 2 is never a full divisor of $\operatorname{qrad}(m)$, and that $\operatorname{qrad}(\operatorname{qrad}(m)) = \operatorname{qrad}(m)$. The condition $d = \operatorname{qrad}(d)$ will mean that d is divisible by no square other than 1 or 4, and that either d is odd, or $4|d$.

The number δ defined in the introduction (cf. (0.5)) can now be described by saying that δ is the largest number such that

$$\delta^2|n \quad \text{and} \quad \delta = \operatorname{qrad}(\delta).$$

For each $M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathbf{T}$, we now define

$$e(M) = \frac{d}{(\operatorname{qrad}(a, d))}.$$

Thus $e(M) = 1$ will mean that $d|\operatorname{qrad}(a)$, and, under the assumption that $ad|n$, we see that $e(M) = 1$ if and only if we can write $a = a'd$, where $a'd^2|n$ and $d = \operatorname{qrad}(d)$.

We set

$$\mathscr{H}' = \{\langle M\rangle |\ M \in \mathbf{T},\ \operatorname{lev}(M)|n \text{ and } e(M) = 1\}$$
$$= \left\{\langle M\rangle \,\middle|\, M = \begin{pmatrix} ad & b \\ 0 & d \end{pmatrix},\ (a, b, d) = 1,\ 0 \leqslant b < d,\ ad^2|n,\ d = \operatorname{qrad}(d)\right\}.$$

We shall show in this section that $\mathscr{H}'$ is a multiplicatively spanning set for $\mathscr{G}$. In the next section we shall show that we get a multiplicative basis by choosing specific values for b. We let

$$\mathscr{H}''_1 = \left\{\left\langle \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right\rangle \in \mathscr{H}' \,\middle|\, b \text{ is a quadratic residue modulo } d\right\},$$

and, when $8|d$, we set $d = 8d_0$, where d_0 is odd, and let

$$\mathscr{H}''_{3,7} = \left\{\left\langle \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right\rangle \in \mathscr{H}' \,\middle|\, 8|d,\ b \text{ is a quadratic residue modulo } d_0, \text{ and } b \equiv 3 \text{ or } 7 \pmod 8\right\},$$

and, finally,

$$\mathscr{H}'' = \mathscr{H}''_1 \cup \mathscr{H}''_{3,7}.$$

Some comments on the nature of the functions in $\mathscr{H}'$ and $\mathscr{H}''$ are in order. When $d = 1$, the function $\langle M\rangle$ is simply $\eta(a\tau)$, so these are always included in $\mathscr{H}'$ and $\mathscr{H}''$ for any $a|n$, and there will be no others when n is divisible by no square other than 1 or 4. When we satisfy the condition $d|a$, as is true for all of the functions in $\mathscr{H}$ and $\mathscr{H}'$ we set $a = a'd$, and the product involved in $\langle M\rangle$ is somewhat simpler than in general:

$$\langle M\rangle = \prod_{c \sim b \pmod d} \eta(a'\tau + c/d).$$

When there is some square $d^2|n$, the functions chosen for $\mathscr{H}'$ are chosen so that d is as small as possible, and consequently the length of the product in

$$\langle M\rangle = \prod_{b \sim 1 \pmod d} \eta(a\tau + b/d)$$

is relatively short. The level of the transforms in this product is ad^2, and $\mathscr{H}'$ contains as many functions of small level as is possible. Thus $\mathscr{H}'$ has been chosen

so that the functions involved are as simple as possible. On the other hand, although $\mathscr{H}''$ is multiplicatively independent, this is not always an advantage. There is some asymmetry forced when we neglect the residues which are not quadratic in its definition, and there are some advantages to be gained, for instance, on $\Gamma_0(25)$, by considering both

$$\left\langle \begin{pmatrix} 5 & 1 \\ 0 & 5 \end{pmatrix} \right\rangle = \eta(\tau+\tfrac{1}{5})\eta(\tau+\tfrac{4}{5}) \quad \text{and} \quad \left\langle \begin{pmatrix} 5 & 2 \\ 0 & 5 \end{pmatrix} \right\rangle = \eta(\tau+\tfrac{2}{5})\eta(\tau+\tfrac{3}{5});$$

one must use more complicated exponents to make some constructions with one of these left out. So we might advise considering working with $\mathscr{H}'$ instead of $\mathscr{H}''$ unless there is some definite benefit to be derived from the multiplicative independence.

Proof that $\mathscr{H}'$ spans $\mathscr{G}$ multiplicatively. We show that if $ad|n$, $M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \boldsymbol{T}$, and $e(M) > 1$, then there are $\langle M_1\rangle, \langle M_2\rangle \in \mathscr{H}$ such that $e(M_i) < e(M)$ and such that

$$\langle M\rangle = \sim \langle M_1\rangle^{\alpha}\langle M_2\rangle^{\beta} \tag{8.2}$$

for some integers α and β. Then a proof by induction on $e(M)$ will show that we can eliminate from $\mathscr{H}$ all of the functions for which $e(M) > 1$, without losing the property of being a multiplicatively spanning set for $\mathscr{G}$ and thus $\mathscr{H}'$ will be such a set.

So suppose $e(M) > 1$ and choose p a prime such that $p|e(M)$. We take C as in (8.1), let $d' = d/p$, and set

$$C' = \{c' \mid 0 \leqslant c' < d' \text{ and } c' \sim b \,(\mathrm{mod}\,(a, d'))\},$$

and choosing some $b' \in C'$, we set $M' = \begin{pmatrix} a & b' \\ 0 & d' \end{pmatrix}$.

We use the following cases of Lemma 4.4:

$$\prod_{k=0}^{p-1} \eta|\begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix} = \sim \eta^{p+1}\cdot(\eta|p)^{-1}, \quad \text{for } p \text{ a prime,}$$

$$\prod_{k=0}^{3} \eta|\begin{pmatrix} 1 & k \\ 0 & r \end{pmatrix} = \sim \eta^{7}\cdot(\eta|2)^{-3} \quad \text{and} \quad \prod_{k=0}^{7} \eta|\begin{pmatrix} 1 & k \\ 0 & 8 \end{pmatrix} = \sim \eta^{15}\cdot(\eta|2)^{-7}. \tag{8.3}$$

Case 1. We consider first the case in which the quadratic classes modulo (a, d') are the same as those modulo (a, d). (The number of quadratic classes is the same in every case, but when $p = 2$ and $4 \nmid d$, then the quadratic classes modulo (a, d') include some even numbers which were not permitted in the quadratic classes modulo (a, d).) In the cases we are considering, each $c \in C$ can be represented uniquely in the form $c = c' + kd'$, where $k = 0, 1, \ldots, p-1$, and $c' \in C'$. Hence, by (8.3),

$$\langle M\rangle = \sim \prod_{c'\in C'}\prod_{k=0}^{p-1} \eta|\begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix}|\begin{pmatrix} a & c' \\ 0 & d' \end{pmatrix} = \sim \prod_{c'\in C'} \eta^{p+1}|\begin{pmatrix} a & c' \\ 0 & d' \end{pmatrix} \Big/ \prod_{c'\in C'} \eta|\begin{pmatrix} pa & pc' \\ 0 & d' \end{pmatrix}$$

$$= \langle M_1\rangle^{p+1} \Big/ \prod_{c'\in C'} \eta|\begin{pmatrix} pa & pc' \\ 0 & d' \end{pmatrix}.$$

Subcase 1a. Suppose $p \nmid d'$. Then with $b'' \equiv pb' \,(\mathrm{mod}\, d')$, we set $M_2 = \begin{pmatrix} pa & b'' \\ 0 & d' \end{pmatrix}$ and we have $\langle M\rangle = \sim \langle M_1\rangle^{p+1}\langle M_2\rangle^{-1}$.

Subcase 1b. Suppose $p|d'$. The matrices $\begin{pmatrix} pa & pc' \\ 0 & d' \end{pmatrix}$ appearing in the denominator of the last expression above are not reduced: the entries have a common factor of p. So we set $d'' = d'/p$, choose some $b'' \equiv b' \,(\mathrm{mod}\, d'')$ with $(a, b'', d'') = 1$, and set $M_2 = \begin{pmatrix} a & b'' \\ 0 & d'' \end{pmatrix}$. The function $\langle M_2\rangle$ involves a product over the index set

$$C'' = \{c'' \mid 0 \leqslant c'' < d'' \text{ and } c'' \sim b'' \,(\mathrm{mod}\,(a, d''))\}.$$

Consider the map $c' \mapsto c''$ of C' onto C'' determined by $c'' \equiv c' \,(\mathrm{mod}\, d'')$. Each $c'' \in C''$ has the same number of preimages in C'; call this number β. Then, since $\eta|\begin{pmatrix} a & c'' \\ 0 & d'' \end{pmatrix} = \sim \eta|\begin{pmatrix} a & c' \\ 0 & d'' \end{pmatrix}$, we have

$$\langle M\rangle = \sim \langle M_1\rangle^{p+1}\langle M_2\rangle^{-\beta}.$$

Case 2. Suppose $p = 2|(a, d)$ and $2 \nmid d'$. Then the map $c \mapsto c'$ determined by $c' \equiv c \,(\mathrm{mod}\, d')$ is a 1-1 correspondence of C onto C' and so we have $\langle M\rangle = \sim \langle M_1\rangle/\langle M_2\rangle$ as in subcase 1a.

9. The multiplicative basis for eta products on $\Gamma_0(n)$. Suppose $M = \begin{pmatrix} ad & b \\ 0 & d \end{pmatrix} \in \boldsymbol{T}$ with $d = \mathrm{qrad}(d)$. Let $d = 2^{\beta}d_0$, where d_0 is odd. If $(b, d) = 1$, we let ν_0 be the number of odd primes p such that b is a quadratic residue modulo p, and set

$$\nu(M) = \nu(d, b) = \begin{cases} \nu_0, & \text{if } \beta = 0, \text{ or} \\ & \quad \beta = 2 \text{ and } b \equiv 1 \,(\mathrm{mod}\, 4), \text{ or} \\ & \quad \beta = 3 \text{ and } b \equiv 1, 3, \text{ or } 7 \,(\mathrm{mod}\, 8), \\ \nu_0 + 1, & \text{otherwise.} \end{cases}$$

Thus $\nu(M)$ counts the number of odd primes p for which b is not a quadratic residue, adding one, in addition, when $4\|d$, $b \equiv 3 \,(\mathrm{mod}\, 4)$ or $8|d$, $b \equiv 5 \,(\mathrm{mod}\, 8)$. Hence we see that $\langle M\rangle \in \mathscr{H}'''$ if and only if $\nu(M) = 0$. We introduce a partial

ordering on

$$\left\{M = \begin{pmatrix} ad & b \\ 0 & d \end{pmatrix} \middle| \; ad^2 | n, \; d = \mathrm{qrad}(d)\right\}$$

by saying

$$M' < M \quad \text{if} \quad \begin{cases} d' | d \text{ and } d' < d, \\ \text{or} \\ d' = d \text{ and } \nu(M') < \nu(M). \end{cases}$$

We shall show that if $\nu(M) > 0$, then there is an identity $\langle M\rangle = \sim \prod_i \langle M_i\rangle^{\alpha_i}$ for some $\alpha_i \in \mathbf{Z}$ and some $M_i < M$. Then $\mathscr{H}''$ will have the same multiplicative span as the set $\mathscr{H}'$, i.e., it will span $\mathscr{G}$ multiplicatively.

Case 1. Suppose there is an odd prime p such that $p|d$ and b is a quadratic non-residue modulo p. Let $d' = d/p$ and choose b' such that $b' \equiv b \pmod{d'}$, $0 \leqslant b' < d$, and $b' \sim 1 \pmod p$. Then $\nu(d, b') = \nu(d', b') = \nu(d, b) - 1$. We set

$$C_0 = \{c|\ 0 \leqslant c < d,\ (d, c) = 1, \text{ and } c \sim b \pmod d\},$$
$$C_1 = \{c|\ 0 \leqslant c < d,\ (d, c) = 1, \text{ and } c \sim b' \pmod d\}, \text{ and}$$
$$C_2 = \{c|\ 0 \leqslant c < d,\ (d, c) = p, \text{ and } c \sim b \sim b' \pmod{d'}\}.$$

Then their union, in terms of d', is

$$C_0 \cup C_1 \cup C_2 = C' = \{c|\ 0 \leqslant c < pd',\ (d', c) = 1, \text{ and } c \sim b' \pmod{d'}\}.$$

We can rewrite C_2 also in terms of d' in the form

$$C_2 = \{pc|\ 0 \leqslant c < d',\ (d', c) = 1, \text{ and } c \sim pb' \pmod{d'}\},$$

so we set $M_1 = \begin{pmatrix} ad & b' \\ 0 & d \end{pmatrix}$, $M_2 = \begin{pmatrix} ad' & pb \\ 0 & d' \end{pmatrix}$, and consider the function h defined by

$$h = \langle M\rangle\langle M_1\rangle\langle M_2\rangle = \prod_{c\in C'} \eta|\begin{pmatrix} ad & c \\ 0 & d \end{pmatrix}.$$

Reducing the elements of C' modulo d' we obtain the set

$$C'' = \{c|\ 0 \leqslant c < d',\ (c, d') = 1, \text{ and } c \sim b' \pmod{d'}\},$$

so that, applying the first equation in (8.3),

$$h = \prod_{c\in C''} \prod_{k=0}^{p-1} \eta|\begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix}|\begin{pmatrix} apd' & c \\ 0 & d' \end{pmatrix}$$
$$= \sim \left[\prod_{c\in C''} \eta|\begin{pmatrix} apd' & c \\ 0 & d' \end{pmatrix}\right]^{p+1} \cdot \left[\prod_{c\in C''} \eta|\begin{pmatrix} ap^2d' & pc \\ 0 & d' \end{pmatrix}\right]^{-1}.$$

Hence, with $M_3 = \begin{pmatrix} apd' & b \\ 0 & d' \end{pmatrix}$, $M_4 = \begin{pmatrix} ap^2d' & pb \\ 0 & d' \end{pmatrix}$, $\alpha_1 = \alpha_2 = \alpha_4 = -1$, and

$\alpha_3 = p+1$, we have $M_i < M$ for each i, and $\langle M\rangle = \prod_i \langle M_i\rangle^{\alpha_i}$, so this case is done.

Case 2. Suppose $b \sim 1 \pmod{d_0}$, $2^\beta = 4$, and $b \equiv 3 \pmod 4$. This is almost identical to case 1, and we omit the argument.

Case 3. Suppose $b \sim 1 \pmod{d_0}$, $2^\beta = 8$, and $b \equiv 5 \pmod 8$. We choose b_1, b_2, and b_3 so that $b_i \equiv b \pmod{d_0}$ and so that $b_1 \equiv 1$, $b_2 \equiv 3$, and $b_3 \equiv 7 \pmod 8$, and define $M_i = \begin{pmatrix} ad & b_i \\ 0 & d \end{pmatrix}$. Consider the product

$$\langle M\rangle\langle M_1\rangle\langle M_2\rangle\langle M_3\rangle = \prod_{c\in C'} \eta|\begin{pmatrix} ad & c \\ 0 & d \end{pmatrix},$$

where $C' = \{c|\ 0 \leqslant c < d,\ c \sim b \pmod{d_0}$, and c is odd$\}$. We let $C'' = \{c|\ 0 \leqslant c < d, c \sim b \pmod{d_0}$, and c is even$\}$, and multiply both sides by the factors $\eta|\begin{pmatrix} ad & c \\ 0 & d \end{pmatrix}$ where $c \in C''$ to obtain

$$\langle M\rangle\langle M_1\rangle\langle M_2\rangle\langle M_3\rangle \prod_{c\in C''} \prod_{k=0}^{3} \eta|\begin{pmatrix} 1 & k \\ 0 & 4 \end{pmatrix}|\begin{pmatrix} 4ad_0 & c \\ 0 & d_0 \end{pmatrix}$$
$$= \prod_{c\in C_6} \prod_{k=0}^{7} \eta|\begin{pmatrix} 1 & k \\ 0 & 8 \end{pmatrix}|\begin{pmatrix} 8ad_0 & c \\ 0 & d_0 \end{pmatrix},$$

for the set $C_6 = \{c|\ 0 \leqslant c < d_0,\ c \sim b \pmod{d_0}\}$. We apply the second and third equations in (8.3) to obtain

$$\langle M\rangle\langle M_1\rangle\langle M_2\rangle\langle M_3\rangle\langle M_4\rangle^7\langle M_5\rangle^{-3} = \sim \langle M_6\rangle^{15}\langle M_7\rangle^{-7},$$

where

$$M_4 = \begin{pmatrix} 4ad_0 & 2b \\ 0 & d_0 \end{pmatrix}, \quad M_5 = \begin{pmatrix} 8ad_0 & 4b \\ 0 & d_0 \end{pmatrix}, \quad M_6 = \begin{pmatrix} 8ad_0 & b \\ 0 & d_0 \end{pmatrix},$$

and

$$M_7 = \begin{pmatrix} 16ad_0 & 2b \\ 0 & d_0 \end{pmatrix}.$$

This completes case 3.

This covers all of the cases, so we have shown that $\mathscr{H}''$ is a multiplicatively spanning set for $\mathscr{G}$.

To show that it is multiplicatively independent, we note that the number of elements in $\mathscr{H}_0$ is

$$|\mathscr{H}_0| = \sum_{ad=n} \omega_1(n),$$

which is a multiplicative function of n, and that the number of elements in $\mathscr{H}''$ is also a multiplicative function of n, by the Chinese remainder theorem, so we

can check that $|\mathscr{H}_0| = |\mathscr{H}''|$ by checking that it is true for each prime power p^α. We leave this computation to the reader. Then $\mathscr{H}_0$ is multiplicatively independent, and $\mathscr{H}''$ has the same multiplicative span as $\mathscr{H}_0$, so $\mathscr{H}''$ must also be multiplicatively independent.

Thus $\mathscr{H}''$ is a multiplicative basis for $\mathscr{G}$ and Theorem E is proven.

References

[1] Bruce C. Berndt, Anthony J. F. Biagioli and James M. Purtilo, *Ramanujan's modular equations of "large" prime degree*, J. Indian Math. Soc. 51(1987).

[2] J. G. Conway and S. P. Norton, *Monstrous Moonshine*, Bull. London Math. Soc. 11 (1979), 308–339.

[3] Victor G. Kac, *Infinite dimensional Lie algebras*, 2nd ed., Cambridge University Press, Cambridge 1985.

[4] Marvin I. Knopp, *Modular functions in analytic number theory*, Markham Publishing Company, 1985.

[5] Marvin Knopp, Joseph Lehner and Morris Newman, *A bounded automorphic form of dimension zero is constant*, Duke Math. J. 32 (3) (1965), 457–460.

[6] Morris Newman, *Construction and application of a certain class of modular functions*, Proc. London Math. Soc., (3), 7 (1956), 334–350.

[7] — *Construction and application of a certain class of modular functions II*, ibid. 9 (1959), 373–387.

[8] W. H. H. Petersson, *Über Thetareihen zu grossen Untergruppen der rationale Modulgruppe*, Springer-Verlag, Berlin 1972.

[9] Hans Rademacher, *Topics in analytic number theory*, Springer-Verlag, New York 1972.

[10] Bruno Schoeneberg, *Elliptic modular functions, an introduction*, Springer-Verlag, Berlin 1972.

DEPARTMENT OF MATHEMATICS AND STATISTICS
THE UNIVERSITY OF MISSOURI AT ROLLA
Rolla, MO 65401-0249
U.S.A.

Received on 13.4.1988
and in revised form on 18.10.1988 (1812)

ACTA ARITHMETICA
LIV (1990)

An upper bound for the h-range of the postage stamp problem

by

ÖYSTEIN J. RÖDSETH (Bergen)

Dedicated to Professor Ernst S. Selmer on the occasion of his 70th birthday

1. Introduction. For a positive integer h, the *h-range* $n(h, A_k)$ of an integer sequence

$$A_k\colon\ a_0 = 0 < 1 = a_1 < a_2 < \ldots < a_k \tag{1}$$

is the largest n for which each of the integers $0, 1, \ldots, n$ can be written as a sum of h elements of A_k, repetitions being allowed. The *extremal h-range* $n(h, k)$ is given by

$$n(h, k) = \max_{A_k} n(h, A_k).$$

The problem of calculating $n(h, k)$ is by some authors referred to as 'the postage stamp problem', due to a rather obvious combinatorial interpretation. In this note we consider $n(h, k)$ for $k \geqslant 1$ fixed and h large.

By a simple combinatorial argument, Rohrbach [11] showed that

$$n(h, k) < \binom{h+k}{k},$$

so in particular

$$n(h, k) \leqslant \frac{k^{k-1}}{(k-1)!}\left(\frac{h}{k}\right)^k + O(h^{k-1}). \tag{2}$$

On the other hand we have $n(h, k) \geqslant (h/k)^k$ (Stöhr [13]).

For $k \leqslant 3$ we have

$$n(h, k) = c_k\left(\frac{h}{k}\right)^k + O(h^{k-1}),$$

where $c_1 = 1$ (trivial), $c_2 = 1$ (Stöhr [13]), $c_3 = 4/3$ (Hofmeister [4], Klotz [6]). For $k \geqslant 4$, however, it is not even known if such a constant c_k exists. Guy ([3],