

## 2. Modular Forms.

**2.0** In this chapter, I discuss what I need from the theory of modular forms. A general reference is **[Ran]**, though I do things in a slightly different way.

If  $R$  is a commutative ring with identity,  $SL_2(R)$  is the group of all  $2 \times 2$  matrices with entries from  $R$  and determinant one. If  $S$  is also a commutative ring with identity, a homomorphism  $\phi : R \rightarrow S$  (that preserves the identity) induces in the obvious way a homomorphism  $SL_2(\phi) : SL_2(R) \rightarrow SL_2(S)$ . In the fashionable jargon,  $SL_2$  is a functor between the category of commutative rings with identity and the category of groups. Moreover, it is plain that  $SL_2$  preserves products:

$$SL_2(R \times S) \simeq SL_2(R) \times SL_2(S). \quad \mathbf{2.0.0}$$

**2.1** From now on,  $A$  will denote a matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$  and, throughout this and the remaining sections of this chapter,  $N$  will denote an integer greater than two.

Define

$$\Gamma(N) := \{A \in SL_2(\mathbb{Z}) : A \equiv \pm I \pmod{N}\}$$

(which is  $\bar{\Gamma}(N)$  in **[Ran]**), which is a normal subgroup of  $SL_2(\mathbb{Z})$ , and

$$\Gamma_0(N) := \{A \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{N}\},$$

$$\Gamma_1(N) := \{A \in \Gamma_0(N) : a \equiv d \equiv \pm 1 \pmod{N}\},$$

which are subgroups (not normal) of  $SL_2(\mathbb{Z})$ .

I shall need to know the value of

$$\mu(N) := [SL_2(\mathbb{Z}) : \Gamma_1(N)].$$

(Here,  $[ : ]$  denotes the index of a subgroup in a group.) Denote by  $\hat{\Gamma}_1(N)$  the image of  $\Gamma_1(N)$  in  $SL_2(\mathbb{Z}_N)$ . Then

$$\mu(N) = [SL_2(\mathbb{Z}_N) : \hat{\Gamma}_1(N)]. \quad 2.1.0$$

Now the order of  $\hat{\Gamma}_1(N)$  is easy to find. It is

$$\#\hat{\Gamma}_1(N) = 2N \quad 2.1.1$$

(since  $N > 2$ ) and it remains for us to calculate  $\#SL_2(\mathbb{Z}_N)$ . For  $n \in \mathbb{N}$ , let

$$\alpha(n) := \#SL_2(\mathbb{Z}_n).$$

**Lemma**

$$\alpha(mn) = \alpha(m)\alpha(n), \text{ if } m \text{ and } n \text{ are coprime,} \quad 2.1.2$$

$$\alpha(p^{k+1}) = p^3 \alpha(p^k), \text{ if } k > 0, \quad 2.1.3$$

$$\alpha(n) = n^3 \prod_{p|n} (1 - 1/p^2) \quad (\text{the product being over the primes}$$

$$\text{dividing } n) \quad 2.1.4$$

**Proof** 2.1.2 follows from 2.0.0 and the fact that  $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$  when  $m$  and  $n$  are coprime.

**2.1.3:** Let  $K$  be the kernel of the map  $SL_2(\mathbb{Z}_{p^{k+1}}) \rightarrow SL_2(\mathbb{Z}_{p^k})$  induced from the projection  $\mathbb{Z}_{p^{k+1}} \rightarrow \mathbb{Z}_{p^k}$ . Then

$$K = \left\{ \begin{pmatrix} 1 + rp^k & sp^k \\ tp^k & 1 + up^k \end{pmatrix} : 0 \leq r, s, t < p \text{ and } u = 0, \text{ if } r=0, = p-r, \text{ otherwise.} \right\}$$

Clearly,  $\#K = p^3$ , which gives us 2.1.3.

2.1.4: After 2.1.2 and 2.1.3, it remains to show that

$$\alpha(p) = p^3 - p.$$

The matrices in  $SL_2(\mathbb{Z}_p)$  can be divided into three sets:

$$V_1 := \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \beta\gamma \neq 0, -1 \right\}, V_2 := \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \beta\gamma = -1 \right\}$$

and  $V_3 := \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \beta\gamma = 0 \right\}.$

It's easy to see that

$$\#V_1 = (p-1)^2(p-2) \text{ and } \#V_2 = (p-1)(2p-1) = \#V_3,$$

so

$$\alpha(p) = (p-1)^2(p-2) + 2(p-1)(2p-1) = p^3 - p. \quad \square$$

It now follows from 2.1.0, 2.1.1 and 2.1.4 that

$$\mu(N) = \frac{1}{2} N^2 \prod_{p|N} (1 - 1/p^2). \quad 2.1.5$$

## 2.2 Set

$$\mathbb{H} := \{\tau \in \mathbb{C} : \text{Im } \tau > 0\}, \quad \mathbb{Q}^* := \mathbb{Q} \cup \{\infty\}.$$

$\mathbb{Q}^*$  is the set of *cusps*.

If  $A \in SL_2(\mathbb{Z})$  and  $\xi \in \mathbb{H}$  or  $\mathbb{Q}^*$ , it is easy to see that

$$A\xi := \frac{a\xi + b}{c\xi + d} \in \mathbb{H} \text{ (respectively, } \mathbb{Q}^*) \text{ (} A\infty = a/c \text{),}$$

and  $SL_2(\mathbb{Z})$  acts on  $\mathbb{H}$  and (transitively) on  $\mathbb{Q}^*$  in this way. A subgroup  $\Gamma$  of  $SL_2(\mathbb{Z})$  induces equivalence relations on  $\mathbb{H}$  and  $\mathbb{Q}^*$ , points  $\xi$  and  $\xi'$  being  $\Gamma$ -equivalent if  $\xi' = A\xi$ , for some  $A \in \Gamma$ . I denote the equivalence class of  $\xi$  by  $[\xi]_\Gamma$ . The *cusps* of  $\Gamma$  are the members of the set  $\Gamma \backslash \mathbb{Q}^*$  (the  $\Gamma$ -orbits of  $\mathbb{Q}^*$ ).

Note that, if  $x$  and  $y$  are coprime integers and  $A \in SL_2(\mathbb{Z})$ , then  $ax + by$  and  $cx + dy$  are also coprime. So we can identify  $\mathbb{Q}^*$  with the set

$$\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : x \text{ and } y \text{ are coprime and } y \geq 0 \right\}$$

( $\infty$  corresponds to  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ) and the action of  $SL_2(\mathbb{Z})$  on  $\mathbb{Q}^*$  becomes matrix multiplication.

My aim in this section is to identify a complete set of distinct cusps of  $\Gamma_1(N)$

For integers  $a$ ,  $b$  and  $n$ , I write  $a \equiv_n b$  for  $a \equiv b \pmod{n}$ .

#### **Lemma**

*If  $x$ ,  $y$  and  $n$  are integers with  $\gcd(x, y, n) = 1$ , there are*

*coprime integers  $x'$  and  $y'$  with  $x' \equiv_n x$  and  $y' \equiv_n y$ . 2.2.0*

**Proof** Let  $p_1, \dots, p_k$  be the primes that divide both  $y$  and one of  $x + m$

( $-\infty < r < \infty$ ). In particular, suppose  $p_1$  divides both  $y$  and  $x + r_1 n$ . The Chinese

remainder theorem tells us that there's a number  $r$  such that  $r \equiv r_1 + 1 \pmod{p_1}$

for each  $1 \leq i \leq k$ . Take  $x' = x + m$ ,  $y' = y$ .  $\square$

**Lemma**

For  $\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} x' \\ y' \end{pmatrix} \in \mathbb{Q}^*$  and  $n \in \mathbb{Z}$ ,

$$\left[ \begin{pmatrix} x \\ y \end{pmatrix} \right]_{\Gamma(n)} = \left[ \begin{pmatrix} x' \\ y' \end{pmatrix} \right]_{\Gamma(n)} \iff \begin{pmatrix} x \\ y \end{pmatrix} =_n \pm \begin{pmatrix} x' \\ y' \end{pmatrix} \quad 2.2.1$$

**Proof**  $\implies$  is obvious. For  $\impliedby$ , I'll only treat the case  $\begin{pmatrix} x \\ y \end{pmatrix} =_n \begin{pmatrix} x' \\ y' \end{pmatrix}$  the other case being very similar. Suppose first that  $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ . Since  $x'$  and  $y'$  are coprime, there are integers  $r$  and  $s$  such that

$$sx' - ry' = 1.$$

Since  $x' =_n 1$  and  $y' =_n 0$ , it follows that  $s =_n 1$  and  $\therefore$  that the matrix

$$B = \begin{pmatrix} x' & r - rx' \\ y' & s - ry' \end{pmatrix}$$

lies in  $\Gamma(n)$  and  $B \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix}$ . Now, for any  $\begin{pmatrix} x \\ y \end{pmatrix}$ , choose  $T \in \text{SL}_2(\mathbb{Z})$  such that  $T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ . If  $T \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x'' \\ y'' \end{pmatrix}$ ,  $x''$  and  $y''$  are coprime and  $\begin{pmatrix} 1 \\ 0 \end{pmatrix} =_n \begin{pmatrix} x'' \\ y'' \end{pmatrix}$ . So there's a matrix  $B \in \Gamma(n)$  with  $B \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x'' \\ y'' \end{pmatrix}$ . Now  $C = T^{-1}BT$  is in  $\Gamma(n)$ , since  $\Gamma(n)$  is normal, and  $C \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix}$ . □

For  $n \in \mathbb{Z}$ , let  $\bar{m}$  denote the congruence class of  $m \in \mathbb{Z}$  modulo  $n$ . Define

$$\mathbb{Q}^{(n)} := \left\{ \begin{pmatrix} \bar{x} \\ \bar{y} \end{pmatrix} \in \mathbb{Z}_n^2 : \bar{x} \text{ and } \bar{y} \text{ are coprime (in } \mathbb{Z}_n) \right\}$$

(Note that  $\bar{x}$  and  $\bar{y}$  are coprime in  $\mathbb{Z}_n$  exactly when  $\gcd(x, y, n) = 1$ .)  $\text{SL}_2(\mathbb{Z})$  acts on  $\mathbb{Q}^{(n)}$ , as on  $\mathbb{Q}^*$ , by matrix multiplication and there's a map  $\mathbb{Q}^* \xrightarrow{\alpha} \mathbb{Q}^{(n)}$  (reduce components modulo  $n$ ) which, by 2.2.0, is surjective.  $\alpha$  commutes with the action of  $\text{SL}_2(\mathbb{Z})$  and so, for any subgroup  $\Gamma \subseteq \text{SL}_2(\mathbb{Z})$ , induces a map  $\Gamma \backslash \alpha : \Gamma \backslash \mathbb{Q}^* \rightarrow \Gamma \backslash \mathbb{Q}^{(n)}$ . 2.2.1 shows that  $\Gamma \backslash \alpha$  is injective, when  $\Gamma(n) \subseteq \Gamma$ , and so we have

**Lemma**

Suppose  $\Gamma(n) \subseteq \Gamma \subseteq SL_2(\mathbb{Z})$ . Then  $\Gamma \backslash \alpha$  is an isomorphism between

the set of cusps of  $\Gamma$  and  $\Gamma \backslash \mathbb{Q}^{(n)}$ .

□

2.2.2

(This result appears in [S, p.11], though the author inadvertently fails to mention the "mod  $n$ " aspect.)

I now describe the set of cusps of  $\Gamma_1(N)$ .

**Theorem**

Suppose  $N > 2$  and define

$$C^{(N)} = \bigcup_{d|N} C_d^{(N)}$$

where

$$C_d^{(N)} = \left\{ \left[ \begin{pmatrix} x \\ y \end{pmatrix} \right]_{\Gamma_1(N)} \in \Gamma_1(N) \backslash \mathbb{Q}^{(N)} : \gcd(y, N) = d \right.$$

$$\text{and } 0 < x < \frac{1}{2}d, 0 \leq y < N$$

$$\text{or } x = \frac{1}{2}d, 0 \leq y \leq \frac{1}{2}N$$

$$\text{or } x = 0, 0 < y < \frac{1}{2}N \}.$$

Then  $C^{(N)}$  may be identified (via the map  $\Gamma_1(N) \backslash \alpha$  of 2.2.2)

with the set of cusps of  $\Gamma_1(N)$ .

2.2.3

**Proof** Suppose  $\left( \begin{pmatrix} x \\ y \end{pmatrix} \right) \in \mathbb{Q}^{(N)}$  and  $\gcd(y, N) = d$ . The subgroup of  $\mathbb{Z}_N$  generated by  $y$  has smallest generator  $\gcd(N, y) = d$ . This means that there are unique integers  $x' = \varepsilon x + ry + sN$  and  $y' = \varepsilon y + tN$  ( $\varepsilon = \pm 1$ ,  $r, s$  and  $t$  integers) such that

$$0 < x' < \frac{1}{2}d \text{ and } 0 \leq y' < N$$

$$\text{or } x' = 0, 0 < y' < \frac{1}{2}N$$

$$\text{or } x' = \frac{1}{2}d \text{ and } 0 \leq y' \leq \frac{1}{2}N$$

Plainly  $\gcd(y', N) = d$ . Now the matrix  $\begin{pmatrix} \varepsilon & r \\ 0 & \varepsilon \end{pmatrix}$  lies in  $\Gamma_1(N)$  and carries  $\begin{pmatrix} x \\ y \end{pmatrix}$  to  $\begin{pmatrix} x' \\ y' \end{pmatrix}$  and so each member of  $\Gamma_1(N) \backslash \mathbb{Q}^{(N)}$  has a representative with the stated properties. The uniqueness of such a representative follows from the uniqueness of the integers  $x'$  and  $y'$  cited above.  $\square$

**2.3** Suppose  $G$  is a group acting on a set  $S$ . For  $s \in S$ , let  $G_s$  denote the subgroup of  $G$  of elements that fix  $s$ . Suppose  $H$  is a subgroup of  $G$ . If  $s \in S$ , define the *width of  $s$  relative to  $H$*  to be

$$w(s; H) := [G_s : H_s].$$

Note that, if  $s$  and  $t$  are  $H$ -equivalent,  $w(s; H) = w(t; H)$ . So we can talk about the width of an orbit of  $H$ .

Now suppose  $G$  acts transitively on  $S$  and let  $T \subseteq S$  be a complete set of distinct representatives of  $H \backslash S$ . While I don't actually need the next result, I have found it useful, for example in checking that I have found all the cusps of a subgroup of  $SL_2(\mathbb{Z})$ . In this lemma,  $[G : H]$  denotes ambiguously the set of right cosets of  $H$  in  $G$  and the number thereof.

**Lemma**

With the above hypothesis and notation, there is a bijection

$$\alpha : [G : H] \longrightarrow \bigcup_{t \in T} [G_t : H_t].$$

As a consequence, if  $[G : H]$  is finite, then each  $w(s; H)$  is finite and

$$\sum_{\zeta \in H \setminus S} w(\zeta; H) = [G : H].$$

**Proof** Pick  $* \in S$  and, for each  $s \in S$ , pick  $x_s \in G$  with  $x_s * = s$  and so that  $x_s x_{s'}^{-1}$  lies in  $H$  whenever  $s$  and  $s'$  are in the same orbit of  $H$ . Such a choice is plainly always possible. I define  $\alpha$  by

$$\alpha(Hg) := H_t x_t x_s^{-1} g x_t^{-1},$$

where  $g* = s = ht$  with  $t \in T$  and  $h \in H$ . Then  $\alpha$  is a well-defined bijection, with inverse

$$H_t g_t \longmapsto H g_t x_t$$

(where  $g_t \in G_t$ ).



$\alpha$  is, of course, far from natural.

$SL_2(\mathbb{Z})$  acts transitively on  $\mathbb{Q}^*$ . If  $\Gamma$  is a subgroup of  $SL_2(\mathbb{Z})$  and  $\zeta \in \Gamma \backslash \mathbb{Q}^*$  is a cusp of  $\Gamma$ , the width of  $\zeta$  relative to  $\Gamma$  is  $w(\zeta; \Gamma)$ , as defined above. Now  $SL_2(\mathbb{Z})_\infty$  is the group  $\langle U, -U \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}$ , where  $U := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ , so, if  $\zeta \in \mathbb{Q}^*$  and  $\zeta = T\infty$ , with  $T \in SL_2(\mathbb{Z})$ ,  $SL_2(\mathbb{Z})_\zeta = \langle TUT^{-1}, -TUT^{-1} \rangle$ . If  $\Gamma$  contains  $-I$ , it is plain that

$$w(\zeta; \Gamma) = \text{the smallest positive integer } k \text{ with } TU^k T^{-1} \in \Gamma. \quad 2.3.0$$



I now give the widths of the various cusps of  $\Gamma_1(N)$ . Recall 2.2.3, that the cusps of  $\Gamma_1(N)$  lie in various sets  $C_d^{(N)}$ , where  $d|N$ .

**Lemma**

*If  $N \neq 4$ , each cusp in  $C_d^{(N)}$  has width  $N/d$ . The same is true when  $N = 4$ , except that the cusp  $1/2$  has width 1.* 2.3.1

**Proof** Take  $N \neq 4$ . Suppose  $\zeta = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Q}^*$  is (a representative of) a cusp of  $\Gamma_1(N)$  lying in (identified with) a member of  $C_d^{(N)}$ . Then  $\gcd(y, N) = d$ . Choose a matrix  $T = \begin{pmatrix} x & u \\ y & v \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$  carrying  $\infty$  to  $\zeta$ . Suppose

$$TU^kT^{-1} = \begin{pmatrix} \varepsilon - kxy & kx^2 \\ -ky^2 & \varepsilon + kxy \end{pmatrix}$$

( $\varepsilon = \pm 1$ ) lies in  $\Gamma_1(N)$ . Then  $N|ky^2$  and  $N|kxy$ , which means (since  $x$  and  $y$  are coprime) that  $N|ky$ . It follows that  $N/d|k$ . On the other hand, it is clear that  $TU^{N/d}T^{-1} \in \Gamma_1(N)$ . The exceptional case when  $N = 4$  is easily verified. □

**2.4** The *Dedekind eta function*,  $\eta$ , is defined on  $\mathbb{H}$  by

$$\begin{aligned} \eta(\tau) &:= \exp(\pi i \tau / 12) \prod_{n=1}^{\infty} (1 - \exp(2\pi i n \tau)) \\ &= q^{1/24}(q)_{\infty}, \end{aligned}$$

where  $q := \exp(2\pi i \tau)$ . If  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ , we have [Kno, thm 2.2, p. 51]

$$\eta(A\tau) = e(A; \tau) \eta(\tau) = \varepsilon(A) \sqrt{c\tau + d} \eta(\tau), \quad \text{2.4.0}$$

for  $\tau \in \mathbb{H}$ , where  $\varepsilon(A)$  is a certain 24th. root of unity (independent of  $\tau$ ). To give the value of  $\varepsilon(A)$ , define the symbols

$$\left(\frac{c}{d}\right)^* := \left(\frac{c}{|d|}\right)$$

$$\left(\frac{c}{d}\right)_* = \left(\frac{c}{|d|}\right), \text{ if } c \geq 0 \text{ or } d > 0, -\left(\frac{c}{|d|}\right) \text{ otherwise}$$

for coprime integers  $c$  and  $d$ , with  $d$  odd, where  $\left(\frac{\bullet}{\bullet}\right)$  is the *Legendre-Jacobi* symbol [H+W. §6.5]. Then

$$\varepsilon(A) = \begin{cases} \left(\frac{d}{c}\right)^* \exp(\pi i/12) ((a+d)c + bd(1-c^2) - 3c), & c \text{ odd,} \\ \left(\frac{c}{d}\right)_* \exp(\pi i/12) ((a+d)c + bd(1-c^2) + 3d(1-c) - 3), & d \text{ odd.} \end{cases} \quad 2.4.1$$

(taking the value of the square root with  $-\pi/2 \leq \arg \sqrt{c\tau + d} < \pi/2$ ).

Suppose that  $\mathfrak{f}$  is any complex valued function defined on  $\mathbb{H}$ . For  $k$  an integer and  $A \in \mathrm{SL}_2(\mathbb{Z})$ , define the function  $(\mathfrak{f}|_k A)$  on  $\mathbb{H}$  by

$$(\mathfrak{f}|_k A)(\tau) := e(A; \tau)^{-k} \mathfrak{f}(A\tau).$$

It follows easily from 2.4.0 that, if  $B$  is also in  $\mathrm{SL}_2(\mathbb{Z})$ ,

$$(\mathfrak{f}|_k AB) = ((\mathfrak{f}|_k A)|_k B) \quad 2.4.2$$

2.4.0 also shows that, with  $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ,

$$e(U^h; \tau) = u, \text{ a 24th root of unity.} \quad 2.4.3$$

(in fact, from 2.4.1,  $u = \exp(\pi i h/12)$ ).

Now suppose  $\Gamma$  is a subgroup of  $\mathrm{SL}_2(\mathbb{Z})$ , of finite index and that  $\mathfrak{f}$  is a function meromorphic on  $\mathbb{H}$  that also satisfies

$$(\mathfrak{f}|_k A) = \chi_{\mathfrak{f}}(A) \mathfrak{f} \quad 2.4.4$$

for every  $A \in \Gamma$ , where each  $\chi_f(A)$  is a root of unity. (If 2.4.4 holds, then, as the notation suggests,  $\chi_f$  is a character on  $\Gamma$ . I leave the proof as an easy exercise for the reader.) Suppose  $\zeta$  is a cusp of  $\Gamma$  of width  $h$  and take  $T \in \text{SL}_2(\mathbb{Z})$  with  $T\infty = \zeta$ . Then

$$\begin{aligned}
 (f|_k T)(\tau+h) &= (f|_k T)(U^h \tau) \\
 &= u^k ((f|_k T)|_k U^h) && \text{(with } u \text{ as at 2.4.3)} \\
 &= u^k (f|_k T U^h)(\tau) && \text{(by 2.4.2)} \\
 &= u^k (f|_k V T)(\tau) && \text{(where } V = T U^h T^{-1} \in \Gamma, \\
 &&& \text{by 2.3.0)} \\
 &= u^k ((f|_k V)|_k T)(\tau) && \text{(2.4.2 again)} \\
 &= u^k \chi_f(A) (f|_k T)(\tau) && \text{2.4.5}
 \end{aligned}$$

If we now set  $u^k \chi_f(V) = \exp(2\pi i r)$  ( $0 \leq r < 1$ ) and define the function  $g$  by

$$g(\tau) := \exp(-2\pi i r \tau / h) (f|_k T)(\tau),$$

2.4.5 shows that  $g$  is invariant under  $\tau \mapsto \tau + h$ . Now suppose  $g$  is holomorphic in a region  $\text{im } \tau > \delta > 0$  (equivalently,  $f$  is holomorphic inside a horocycle at  $\zeta$ ). Then  $g$  has a Fourier series expansion

$$g(\tau) = \sum_n a_n q_h^n,$$

where  $q_h := \exp(2\pi i \tau / h)$ , and  $\therefore$

$$(f|_k T)(\tau) = q_h^{-r} \sum_n a_n q_h^n. \quad \text{2.4.6}$$

$f$  is *meromorphic* at the cusp  $\zeta$  if  $f$  is holomorphic inside a horocycle at  $\zeta$  and if the series in 2.4.6 is finite on the left. If this is so and if  $m$  is the smallest integer with  $a_m \neq 0$ , the *order* of  $f$  at  $\zeta$  (with respect to  $\Gamma$ ) is

$$\text{ord}(\mathfrak{f}, \zeta, \Gamma) := r + m.$$

This number is independent of the choice of  $T$  with  $T_\infty = \infty$  (a different choice merely multiplies 2.4.6 by a root of 1) and furthermore

$$\text{ord}(\mathfrak{f}, \xi, \Gamma) = \text{ord}(\mathfrak{f}, \zeta, \Gamma),$$

when  $\zeta$  and  $\xi$  are  $\Gamma$ -equivalent. So we can speak of the order of  $\mathfrak{f}$  at a cusp of  $\Gamma$ .

I now define a *modular form of weight  $k/2$*  on  $\Gamma$  to be a function that satisfies 2.4.4 and is meromorphic on  $\mathbb{H}$  and at the cusps. So  $\eta$  is a modular form of weight  $1/2$  on  $SL_2(\mathbb{Z})$  ( $SL_2(\mathbb{Z})$  has just one cusp at  $\infty$  and  $\eta$  is visibly meromorphic there). The following result, a simple corollary of a theorem due to Rankin [Ran, thm. 4.1.4] is the linch-pin of my proofs of theorems D, E and H:

#### Theorem

Suppose  $\Gamma$  is a subgroup of  $SL_2(\mathbb{Z})$  of index  $\mu$  and that  $\Gamma$  contains  $-I$ . If  $\mathfrak{f}$  is a modular form of weight  $r$  on  $\Gamma$  that is holomorphic on  $\mathbb{H}$  and not identically zero then,

$$\sum_{\alpha \in \Gamma \backslash \mathbb{Q}^*} \text{ord}(\mathfrak{f}, \alpha, \Gamma) \leq \mu r / 12. \quad \square \quad 2.4.7$$

2.5 For positive integers  $n$ , define functions  $\eta(n) = \eta(n; \tau)$  on  $\mathbb{H}$  by:

$$\eta(n; \tau) := \eta(n\tau) = \eta(L_n \tau),$$

where  $L_n := \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$ . For  $A \in \Gamma_0(n)$ , define

$$A^{(n)} := L_n A L_n^{-1} = \begin{pmatrix} a & nb \\ c/n & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Now, for  $A \in \Gamma_0(n)$ ,

$$\eta(n; A\tau) = \eta(L_n A\tau) = \eta(A^{(n)} L_n \tau) = \varepsilon(A^{(n)}) \sqrt{c\tau+d} \eta(n; \tau),$$

so

$$(\eta(n) |_1 A) = \phi(\eta(n); A) \eta(n)$$

where

$$\phi(\eta(n); A) = \varepsilon(A^{(n)}) \varepsilon(A)^{-1} \quad 2.5.0$$

and  $\eta(n)$  is a modular form of weight  $1/2$  on  $\Gamma_0(n)$

Rademacher [Rad, 81.2, p.181] defines functions

$$\Theta_{\mu, \nu}(v | \tau) := \sum_{n=-\infty}^{\infty} (-)^{vn} \exp((n+\mu/2)^2 \pi i \tau) \exp(2\pi i (n+\mu/2)v)$$

and shows that

$$\Theta_{1,1}(v | A\tau) = \varepsilon(A)^3 \exp(\pi i c v^2 (c\tau+d)) \sqrt{c\tau+d} \Theta_{1,1}(v(c\tau+d) | \tau) \quad 2.5.1$$

$$\begin{aligned} \Theta_{1,0}(v | A\tau) &= i^{1-d} \exp(\pi i c d / 4) \varepsilon(A)^3 \exp(\pi i c v^2 (c\tau+d)) \\ &\quad \times \sqrt{c\tau+d} \Theta_{1-c, 1-d}(v(c\tau+d) | \tau) \end{aligned} \quad 2.5.2$$

(Here, Rademacher has  $\sqrt{(c\tau+d)/i}$  where I have  $\sqrt{c\tau+d}$ , so his expressions look a little different.)

Note the obvious

$$\Theta_{\mu+2, \nu}(v | \tau) = (-)^{\nu} \Theta_{\mu, \nu}(v | \tau), \quad \Theta_{\mu, \nu+2}(v | \tau) = \Theta_{\mu, \nu}(v | \tau)$$

(so that really there are only four functions  $\Theta_{\mu, \nu}$ ) and

$$\Theta_{1,1}(v+1 | \tau) = -\Theta_{1,1}(v | \tau), \quad \Theta_{1,0}(v+1 | \tau) = -\Theta_{1,0}(v | \tau). \quad 2.5.3$$

For integers  $n > 0$  and  $k$ , define functions  $s_n(k)$  and  $t_n(k)$  on  $\mathbb{H}$  by

$$s_n(k; \tau) := -\exp(\pi i k^2 \tau / n) \Theta_{1,1}(k\tau | n\tau) = q^{(n/2-k)^2/2n} [q^k; q^n]_{\infty} (q^n)_{\infty}$$

$$t_n(k; \tau) := \exp(\pi i k^2 \tau / n) \Theta_{1,0}(k\tau | n\tau) = q^{(n/2-k)^2/2n} [-q^k; q^n]_{\infty} (q^n)_{\infty}$$

These functions  $s_n(k)$  and  $t_n(k)$  and the fact that, as I shall soon show, they are modular forms on  $\Gamma_1(n)$  and  $\Gamma_1(2n)$  respectively must be well known, but I've found no reference to them in the published literature. I got the idea from [Gar2'], in which the author introduces certain special cases of these functions (see §0.5).

Note that

$$s_n(-k) = -s_n(k) = s_n(k+n) \quad 2.5.4$$

$$t_n(-k) = t_n(k) = t_n(k+n) \quad 2.5.5$$

and that

$$\exp(\pi i k^2 \tau / n) \Theta_{0,0}(k\tau | n\tau) = t_n(n/2 - k; \tau) \quad 2.5.6$$

For a function  $f$  of  $x$  of the form  $f(x) = x^r(a_0 + a_1x + a_2x^2 + \dots)$  with  $a_0 \neq 0$  and  $r$  rational, define:  $\text{ord } f := r$ . Now, writing  $\lambda_n(k)$  for the least nonnegative residue of  $k$  modulo  $n$ , 2.5.4 and 2.5.5 and the definitions of these functions show that

$$\text{ord } s_n(k) = (n/2 - \lambda_n(k))^2/2n = \text{ord } t_n(k) \quad 2.5.7$$

Now, if  $A \in \Gamma_0(n)$ , we have, with the help of 2.5.1,

$$\begin{aligned}
s_n(k; A\tau) &= -\exp(\pi i k^2 A\tau/n) \Theta_{1,1}(kA\tau | L_n A\tau) \\
&= -\exp(\pi i k^2 A\tau/n) \Theta_{1,1}(kA\tau | A^{(n)} L_n \tau) \\
&= -\epsilon(A_n)^3 \exp(\pi i k^2 A\tau/n) \exp(\pi i (kA\tau)^2 (c/n)(c\tau+d)) \sqrt{c\tau+d} \\
&\quad \times \Theta_{1,1}(kA\tau(c\tau+d) | L_n \tau) \\
&= -\epsilon(A_n)^3 \exp(\pi i (k^2 A\tau/n)(1 + c(a\tau+b)) \sqrt{c\tau+d}) \Theta_{1,1}(k(a\tau+b) | n\tau) \\
&= -\epsilon(A_n)^3 \exp(\pi i k^2 a(a\tau+b)/n) \sqrt{c\tau+d} (-)^{kb} \Theta_{1,1}(ka\tau | n\tau)
\end{aligned}$$

(where I've used 2.5.3 and the fact that  $1+bc = ad$ )

$$= (-)^{kb} \epsilon(A^{(n)})^3 \exp(\pi i k^2 ab/n) \sqrt{c\tau+d} s_n(ak; \tau). \quad 2.5.8$$

Thus, for  $A \in \Gamma_0(n)$ ,

$$(s_n(k) |_1 A) = \sigma(s_n(k); A) s_n(ak), \quad 2.5.9$$

where

$$\sigma(s_n(k); A) = (-)^{kb} \exp(\pi i k^2 ab/n) \epsilon(A^{(n)})^3 \epsilon(A)^{-1}. \quad 2.5.10$$

Working in the same way with 2.5.2, we have, for  $A \in \Gamma_0(n)$ , that

$$\begin{aligned}
(t_n(k) |_1 A) &= \sigma(t_n(k); A) t_n(ak), \text{ if } A \in \Gamma_0(2n) \\
&= \sigma(t_n(k); A) t_n(n/2 - ak), \text{ if } A \in \Gamma_0(2n) \text{ and } n \text{ is even.}
\end{aligned} \quad 2.5.11$$

where

$$\sigma(t_n(k); A) = (-)^{kb} i^{1-d} \exp(\pi i cd/4n) \exp(\pi i k^2 ab/n) \epsilon(A^{(n)})^3 \epsilon(A)^{-1} \quad 2.5.12$$

2.5.4, 2.5.5, 2.5.9 and 2.5.11 show that  $s_n(k)$  and  $t_n(k)$  are modular forms of weight  $1/2$  on  $\Gamma_1(n)$ , respectively  $\Gamma_1(2n)$  (that these functions are meromorphic at the cusps will be shown in the next section).

For an  $\alpha$ -tuple  $\mathbf{l} = (l_0, \dots, l_{\alpha-1})$  with integral entries, set  $\text{len } \mathbf{l} = \alpha$  and define

$$s_n(\mathbf{l}) = \prod_{r=0}^{\alpha-1} s_n(l_r).$$

Define  $t_n(\mathbf{l})$  and  $\eta(\mathbf{l})$  in the same way and, for even  $n$ , define

$$t'_n(\mathbf{l}) = \prod_{r=0}^{\alpha-1} t_n(n/2 - l_r).$$

In sections 3.1-3 I shall be dealing with functions of the form

$$\mathcal{X}(\mathbf{m}) = \frac{s_n(\mathbf{u})t_n(\mathbf{v})\eta(\mathbf{b})}{s_n(\mathbf{x})t_n(\mathbf{y})\eta(\mathbf{c})} \quad 2.5.13$$

in which  $\mathbf{u}$ ,  $\mathbf{v}$ ,  $\mathbf{x}$  and  $\mathbf{y}$  are linearly dependent on the parameters  $\mathbf{m}$  and in which entries of  $\mathbf{b}$  and of  $\mathbf{c}$  (which will be independent of  $\mathbf{m}$ ) are positive integers dividing  $n$ . Set

$$w := \text{len } \mathbf{u} + \text{len } \mathbf{v} + \text{len } \mathbf{b} - \text{len } \mathbf{x} - \text{len } \mathbf{y} - \text{len } \mathbf{c}. \quad 2.5.14$$

Then, for  $A \in \Gamma_0(n)$  ( $n$  even), we have, by 2.5.9 and 2.5.11

$$\begin{aligned} (\mathcal{X}(\mathbf{m})|_w A) &= o(\mathcal{X}(\mathbf{m}); A) \mathcal{X}(\mathbf{am}), \text{ if } A \in \Gamma_0(2n), \\ &= o(\mathcal{X}(\mathbf{m}); A) \mathcal{X}'(\mathbf{am}), \text{ if } A \in \Gamma_0(2n), \end{aligned} \quad 2.5.15$$

where

$$\begin{aligned} o(\mathcal{X}(\mathbf{m}); A) &= o(s_n(\mathbf{u}); A) o(t_n(\mathbf{v}); A) o(\eta(\mathbf{b}); A) \\ &\quad \times o(s_n(\mathbf{x}); A)^{-1} o(t_n(\mathbf{y}); A)^{-1} o(\eta(\mathbf{b}); A)^{-1} \end{aligned}$$

and  $\mathcal{X}'(\mathbf{am})$  is  $\mathcal{X}(\mathbf{am})$ , with  $t'_n$  for  $t_n$ .

I shall call a function like  $\mathcal{X}(\mathbf{m})$  at 2.5.13 or  $\mathcal{X}'(\mathbf{m})$  a *theta product* of *index*  $n$ , whose *weight* is  $w/2$  ( $w$  as defined at 2.5.14). If  $\mathcal{X}(\mathbf{m})$  and  $\mathcal{Y}(\mathbf{m})$  are theta products of the same weight and same index ( $n$ , say), and if  $o(\mathcal{X}(\mathbf{m}); A) =$



$\nu(Y(m); A)$  for all  $A \in \Gamma_0(2n)$ , I shall say that  $X(m)$  and  $Y(m)$  are *compatible*.

Suppose  $X(m)$  and  $Y(m)$  are compatible. Then  $Z(m) = X(m) + Y(m)$  transforms according to

$$(Z(m) |_{\mathbf{w}} A) = \nu(Z(m); A) Z(am),$$

for every  $A \in \Gamma_0(2n)$ , where  $\nu(Z(m); A) = \nu(X(m); A)$ .

Define the *sign* of the theta product  $X(m)$  to be  $(-)^{\text{len } u + \text{len } x}$  and, for numbers  $a \equiv \pm 1 \pmod{n}$ , define  $\chi_n(a) = \pm 1$  by:

$$\chi_n(a) \equiv a \pmod{n}. \quad 2.5.16$$

Then I say that that theta products  $X(m)$  and  $Y(m)$  are *coherent* if they are compatible, when they have the same sign, and otherwise

$$\nu(X(m); A) = \chi_{2n}(a) \nu(Y(m); A).$$

for every  $A \in \Gamma_1(2n)$ . It is plain that a sum of mutually coherent theta products of index  $n$  and weight  $w/2$  is a modular form of weight  $w/2$  on  $\Gamma_1(2n)$ .

**2.6** In this section, I calculate the orders of the forms  $\eta(r)$ , for  $r|n$ ,  $s_n(k)$  and  $t_n(k)$  at the various cusps of  $\Gamma_1(2n)$ .

Suppose that  $\zeta = x/y \in \mathbb{Q}^*$  with  $\gcd(y, 2n) = \delta$ , so  $\zeta$  represents a cusp in  $C_{\delta}^{(2n)}$ .

Take a matrix  $T = \begin{pmatrix} x & * \\ y & z \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$  that carries  $\infty$  to  $\zeta$ . Suppose  $r|n$  and set

$\delta' = \gcd(r, y)$ ,  $r' = r/\delta'$ ,  $y' = y/\delta'$ . Let  $T^* := \begin{pmatrix} r'x & * \\ y' & z' \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ . Then

$$T^{*-1} L_r T = V := \begin{pmatrix} \delta' & * \\ 0 & r' \end{pmatrix},$$

where  $\delta' = \gcd(y, r)$ , and  $\therefore$

$$\eta(r; T\tau) = \eta(T^*V\tau) = \varepsilon(T^*)\sqrt{(y\tau+z)/r'} \eta(V\tau)$$

and (since, by 2.3.1, cusps in  $C_\delta^{(2n)}$  have width  $2n/\delta$ ) it follows that

$$\text{ord}(\eta(r), \zeta, \Gamma_1(n)) = n\delta'^2/12r\delta. \quad 2.6.0$$

Now calculations similar to those preceding 2.5.8 show that

$$s_n(k; T\tau) = u\sqrt{(y\tau+z)/n'} \exp(\pi i k^2 x(x\tau + *)/n) \Theta_{1,1}(k(x\tau + *)/n' | (\delta'^2\tau + *)/n)$$

where  $u \in \mathcal{U}$ , the  $*$ 's are (unimportant) integers and  $\delta'$ ,  $n'$  (and  $y'$  below) are as above, with  $n$  for  $r$ . It follows from 2.5.7 and 2.3.1 that

$$\begin{aligned} \text{ord}(s_n(k), \zeta, \Gamma_1(2n)) &= \text{ord } s_{\delta'/2/n}(kx/n') \times (2n/\delta) \\ &= (\delta'/2 - \lambda)^2/\delta, \end{aligned} \quad 2.6.1$$

where  $\lambda = \lambda_{\delta'}(kx)$  is the least nonnegative residue of  $kx \bmod \delta'$ .

In the same way, we have

$$t_n(k; T\tau) = u\sqrt{(y\tau+z)/n'} \exp(\pi i k^2 x(x\tau + z)/r) \Theta_{1-y', 1-z'}(k(x\tau + z)/n' | (\delta'^2\tau + *)/n),$$

We can suppose  $z'$  is odd and then

$$\begin{aligned} \text{ord}(t_n(k), \zeta, \Gamma_1(2n)) &= \text{ord } t_{\delta'/2/n}(kx/n') \\ &= (\delta'/2 - \lambda)^2/\delta \quad \text{if } y' \text{ is even,} \\ &= \text{ord } t_{\delta'/2/n}(\delta'^2/2n - kx/n') \\ &= \mu^2/\delta, \quad \text{if } y' \text{ is odd,} \end{aligned} \quad 2.6.2$$

where  $\lambda$  is as above and  $\mu$  satisfies  $kx \equiv \mu \bmod \delta'$  and  $-\delta'/2 < \mu \leq \delta'/2$ .