ACTA ARITHMETICA
IX (1964)

On theta-functions for certain quadratic fields

by

H. Cohn (Tucson, Arizona)

Dedicated to Louis J. Mordell on his seventy-fifth birthday

1. Introduction. In some recent papers [1], [2], [3] it was noted that the problem of finding the number of representations by the form

$$Q_1 = \xi_1^2+\xi_2^2+\xi_3^2+\xi_4^2 \tag{1a}$$

is of unusual interest when the variables ξ_i are integers in the field $Q(\sqrt{3})$, over the rationals Q, particularly since this problem is not quite as simple here as in the case of $Q(\sqrt{5})$, done by Siegel and Götzky [12], [5] or as in the case of $Q(\sqrt{2})$ [1]. The following *unsatisfactory* result was established: Let $R_1(\mu)$ be the number of representations in quadruples $(\xi_1, \xi_2, \xi_3, \xi_4)$ where $\xi_i = a_i+b_i\sqrt{3}$ (a_i, b_i rational integers) of $Q_1 = \mu$ for $\mu = a+2b\sqrt{3}$ and $a > 2|b|\sqrt{3}$. Then we define

$$\begin{aligned} D(\mu) &= \sum_{(\nu)} |N(\nu)| \quad \text{where} \quad (\nu)\,|\,(\mu) \ \text{(in } Q(\sqrt{3})), \\ D^*(\mu) &= \sum_{(\nu)} |N(\nu)| \quad \text{where} \quad (\nu)\,|\,(\mu) \ \text{and} \ N(\mu/\nu) \ \text{is odd}; \end{aligned} \tag{2}$$

(here the sums are limited to ideal divisors so that associates of any ν are not repeated). From these we define the "singular series contribution" [1]

$$B(\mu) = \begin{cases} 4D^*(\mu) & \text{if} \quad 8\nmid N(\mu), \\ 24D(\mu)-42D^*(\mu) & \text{if} \quad 8\,|\,N(\mu). \end{cases} \tag{3}$$

Then the representation function $R_1(\mu)$ for $Q_1 = \mu$ is not quite $B(\mu)$, but rather

$$R_1(\mu) = B(\mu)+4L(\mu) \tag{1b}$$

where $L(\mu)$ is an "unknown" function. Actually the techniques [10] which Mordell introduced for the Ramanujan tau-function make $L(\mu)$

somewhat "accessible" because $L(\mu)$ can be shown to be multiplicative and to vanish "quite often" [2]. In the fields of $\sqrt{2}$ and $\sqrt{5}$, however, an analogue of the term $4L(\mu)$ would not occur [1], [5].

The presence of the term $4L(\mu)$ in (1b) can be accounted for by the classical Siegel "genus theory" [12] as evidence that other forms occur in the genus of Q_1, (say) $Q_2, \ldots$, so that $B(\mu)$ is not $R_1(\mu)$ but a weighted average of the numbers of representations $R_1(\mu), R_2(\mu), \ldots$, of $Q_1 = \mu_1$, $Q_2 = \mu_2, \ldots$ G. Pall [3] showed how the representation problem of $Q_1 = \mu$ can be expressed in rational terms thus transforming the representation problem to the more closely explored rational domain.

Subsequently, M. Kneser (in private communications) pointed out that there are two (and conjecturally only two) additional forms Q_2 and Q_3 in the genus of Q_1, namely

$$Q_2 = \xi_1^2+\xi_2^2+2\xi_3^2+2\sqrt{3}\,\xi_3\xi_4+2\xi_4^2, \tag{4a}$$

$$Q_3 = 3(\xi_1^2+\xi_2^2+\xi_3^2+\xi_4^2)+2(1+\sqrt{3})(\xi_1\xi_3-\xi_2\xi_4)+ \\ +2(1-\sqrt{3})(\xi_1\xi_4+\xi_2\xi_3). \tag{5a}$$

In this paper, we shall verify independently of the Siegel theory that these forms have the representation functions

$$\left.\begin{aligned} R_2(\mu) &= B(\mu) \qquad (4b)\\ R_3(\mu) &= B(\mu)-4L(\mu) \qquad (5b)\end{aligned}\right\} \text{ where } \quad \mu = a+2b\sqrt{3},\ a > 2|b|\sqrt{3}.$$

In fact, without extra effort, we shall note that the *even* form

$$Q_0 = 2\xi_1^2+2\sqrt{3}\,\xi_1\xi_2+2\xi_2^2+2\xi_3^2+2\sqrt{3}\,\xi_3\xi_4+2\xi_4^2 \tag{6a}$$

(which represents only integers μ divisible by 2) has the representation function for $\mu = 2(a+b\sqrt{3})$, $a > |b|\sqrt{3}$,

$$R_0(\mu) = 24D(\mu/2). \tag{6b}$$

We shall use the functional equation of theta-functions avoiding any explicit reference to the genus concept. Indeed, our Main Theorem (§ 4 below) suggests a weaker version of the genus concept which is really the one directly involved in the condition that the functional equation of the theta-functions be satisfied.

2. Terminology of fields and forms. We consider a quadratic field $Q(\sqrt{m})$ where m is a positive square-free integer satisfying $m \equiv 2$ or $3 \pmod 4$. We note $4m = D$ the discriminant of the field. We let $\mathfrak{O}$ denote the ring of algebraic integers $a+b\sqrt{m}$ and we let $\mathfrak{O}_2$ denote the subring

of integers where b is even. We let $\mathfrak{O}^+$ and $\mathfrak{O}_2^+$ denote the semigroups in each of the rings consisting of totally positive integers. The special integers

$$\varepsilon = A+B\sqrt{m} > 1 \tag{7a}$$

and

$$\eta = m+\sqrt{m} \tag{7b}$$

denote the fundamental unit ε and a convenient element η_2 lying in the ideal $\mathbf{2}_1$ but not in the ideal $\mathbf{2}$ (where $\mathbf{2} = \mathbf{2}_1^2$ in Hasse's notation).

We consider positive definite n-ary quadratic (classic) forms having (matrix) coefficients in $\mathfrak{O}$ *and representing only numbers in* $\mathfrak{O}_2$ (actually in $\mathfrak{O}_2^+$ or zero). We write such a form as a bilinear form

$$Q(A, M) = \sum_{i,j} a_{ij}\lambda_i\mu_j \qquad (a_{ij} = a_{ji}) \tag{8a}$$

where $A = (\lambda_1, \ldots, \lambda_n)$, $M = (\mu_1, \ldots, \mu_n)$ are vectors (in $\mathfrak{O}^n$) with components in $\mathfrak{O}$. We call the form

$$Q(A) = Q(A, A), \tag{8b}$$

recalling such identities as

$$Q(A+M) = Q(A)+2Q(A, M)+Q(M), \quad \text{etc.} \tag{9}$$

Clearly a_{ii} must lie in $\mathfrak{O}_2^+$ but a_{ij} merely lies in $\mathfrak{O}$. We call Q' the *conjugate* form (where a'_{ij} replaces a_{ij}).

The standard "canonical" reduction techniques [7] permit a p-adic reduction of a form to t diagonal terms with nondiagonal terms available in the form of blocks of order 2. Actually, we want to define a weaker concept of a *semidiagonalized form* as follows: For some integer t $(0 \leqslant t \leqslant n)$,

$$\begin{aligned} &a_{11} \equiv a_{22} \equiv \ldots \equiv a_{tt} \equiv 1 \pmod{\mathbf{2}_1}, \\ &a_{ij} \equiv 0 \pmod{\mathbf{2}_1} \quad \text{if} \quad 1 \leqslant (i \text{ or } j) \leqslant t \end{aligned} \tag{10a}$$

while the remaining $(n-t)$ by $(n-t)$ matrix represents an even form:

$$a_{t+1,t+1} \equiv \ldots \equiv a_{nn} \equiv 0 \pmod 2. \tag{10b}$$

It is clear from elementary considerations that such a matrix is always obtainable by a unimodular transformation. For example, if $Q(A)$ represents only even numbers, (10b) is valid for $t = 0$; if, however, $Q(A)$ represents an odd number we can arrange to have an odd diagonal coefficient at (say) a_{11} so that the substitution of $\lambda_1+\alpha_{12}\lambda_2+\ldots+\alpha_{1n}\lambda_n$ for λ_1 will

produce the desired congruence property (10a) for the first row and column. We continue with the remaining matrix of the last $(n-1)$ rows and columns until (in t steps) a matrix (of $(n-t)$ rows and columns) constituting an even form is encountered. The canonical reduction theory, of course, informs us that t is well-defined by Q.

We assume all matrices used here are in semidiagonalized form.

We next introduce the vector

$$\Omega_t = (1, \ldots, 1, 0, \ldots, 0) \tag{11}$$

consisting of t unities and $n-t$ zeros as shown.

LEMMA 1. *If $Q(\Lambda)$ is semidiagonalized, then*

$$Q(\Lambda, \Omega_t) \equiv Q(\Lambda) (\mathrm{mod}\, 2_1). \tag{12}$$

The proof follows from the fact that $\lambda \equiv \lambda^2 (\mathrm{mod}\, 2_1)$.

A very important constant which arises here is

$$Q(\Omega_t, \Omega_t) = q \tag{13}$$

which belongs to $\mathfrak{O}_2^+$ and is easily seen to satisfy

$$q \equiv t (\mathrm{mod}\, 2). \tag{14}$$

Of course, q is not well-defined by Q (as is t); we shall see (§ 4 below) that it is determined modulo $2\mathfrak{O}_2$ (and, fortunately, only its value modulo $2\mathfrak{O}_2$ is of significance for us).

In the present illustrations the following values of t and q occur:

$$\begin{aligned} Q_0&: \quad t = 0, \ q = 0, \\ Q_1&: \quad t = 4, \ q = 4, \\ Q_2&: \quad t = 2, \ q = 2, \\ Q_3&: \quad t = 4, \ q = 16 - 4\sqrt{3}. \end{aligned} \tag{15}$$

In all these cases q is the same $(\mathrm{mod}\, 2\mathfrak{O}_2)$.

3. Theta-functions. We now consider two complex variables

$$Z = X + iY, \quad Z' = X' + iY' \quad \text{where} \quad Y' < 0 < Y. \tag{16a}$$

These are called *conjugates* and are treated formally like conjugate quadratic surds (although they are independent "functionally"). Thus the definition on norm and trace is extended to include them formally, e.g., $N(Z) = ZZ'$ (which is not necessarily positive or even real) and $S(\lambda Z) = \lambda Z + \lambda' Z'$ if λ lies in $\mathfrak{O}$, etc. We also define

$$e(\lambda Z) = \exp \pi i S(\lambda Z / 2\sqrt{m}) = \exp \pi i [(\lambda Z - \lambda' Z')/2\sqrt{m}]. \tag{16b}$$

Thus for λ in $\mathfrak{O}$, $e(\lambda) = 1$ if and only if λ lies in $\mathfrak{O}_2$.

Then we define the theta-function corresponding to the quadratic form Q as

$$\Theta_Q(Z, Z') = \sum_{\Lambda \in \mathfrak{O}^n} e[ZQ(\Lambda)] \tag{17}$$

summed over all integral vectors Λ (with corresponding $Q(\Lambda)' = Q'(\Lambda')$). We shall assume all series indicated to be absolutely convergent on the basis of well-known estimates [1]. In particular, the theta-function corresponding to

$$Q^{(n)} = \lambda_1^2 + \ldots + \lambda_n^2 \tag{18}$$

is written as

$$\Theta^{(n)}(Z, Z') = \sum_{\lambda_i \in \mathfrak{O}} e[(\lambda_1^2 + \ldots + \lambda_n^2) Z] \tag{19a}$$

and it has the property that

$$\Theta^{(n)}(Z, Z') = [\Theta^{(1)}(Z, Z')]^n. \tag{19b}$$

We note that Θ_Q is defined independently of the (matrix) basis chosen for the form Q.

We next shall define a certain group $\mathfrak{G}^*$ of linear transformations (with coefficients in $\mathfrak{O}$) preserving the half-planes of Z and Z':

$$Z_1 = \frac{\alpha Z + \beta}{\gamma Z + \delta}, \quad Z_1' = \frac{\alpha' Z' + \beta'}{\gamma' Z' + \delta'}. \tag{20}$$

The definition of $\mathfrak{G}^*$ shall be in terms of generators:

$$\begin{pmatrix} \varepsilon^2 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad (\alpha \text{ arbitrary in } \mathfrak{O}). \tag{21}$$

(We indicate only the matrix for one of the variables (say) Z, the other variable Z' naturally being transformed by the algebraic conjugate.) Evidently $\alpha\delta - \beta\gamma$ in (20) is always the square of a unit in $\mathfrak{O}$.

In many cases, including those $\mathfrak{O}$ possessing the Euclidean algorithm, $\mathfrak{G}^*$ constitutes an important subgroup $\mathfrak{G}$ of the complete Hilbert group Ω consisting of *all* transformations (20) where $\alpha\delta - \beta\gamma$ is the square of a unit. (The complete Hilbert group Ω consists of the transformations (20) where the unit $\alpha\delta - \beta\gamma$ is totally positive, although not necessarily a square when $N(\varepsilon) > 0$.)

In practice we wish to build out of $\Theta_Q(Z, Z')$ a set of conjugates under $\mathfrak{G}^*$; hence, using [1] as a model we form:

$$\Theta_Q(c, d; Z, Z') = \sum_{\Lambda \in \mathfrak{O}^n} e[ZQ(\Lambda + c\eta\Omega_t/2) + dQ(\Lambda, \eta\Omega_t)]. \tag{22}$$

We assume henceforth that in addition to earlier restrictions on Q, the determinant of (the matrix for) Q is a unit in $\mathfrak{O}$. Here we first verify that at most *four* different functions are defined by the rational integers c and d (actually modulo 2), or

$$(23)\qquad \Theta_Q(c+2, d;\ Z, Z') = \Theta_Q(c, d+2;\ Z, Z') = \Theta_Q(c, d;\ Z, Z').$$

To verify this result note that if c is changed to $c+2$ then the net effect is to change Λ in $Q(\Lambda+c\eta\Omega_t/2)$ to $\Lambda+\eta\Omega_t$ (which again spans all of $\mathfrak{O}^n$); furthermore changing Λ to $\Lambda+\eta\Omega_t$ in $Q(\Lambda, \eta\Omega_t)$ produces a change in the argument of $e[\dots]$ by $Q(\eta\Omega_t, \eta\Omega_t) = \eta^2 q$ which lies in $\mathfrak{O}_2$ and therefore produces no change. (Actually this technique is used extensively in the results that follow.)

LEMMA 2. *The conjugates $\Theta_Q(c, d; Z, Z')$ transform as follows under the generators of $\mathfrak{G}^*$:*

$$(24a)\qquad \Theta_Q(c, d;\ Z+1, Z'+1) = \Theta_Q(c, d+c;\ Z, Z')e_1,$$

$$(24b)\qquad \Theta_Q(c, d;\ Z+\eta, Z'+\eta') = \Theta_Q(c, d+1;\ Z, Z')e_2,$$

$$(24c)\qquad \Theta_Q(c, d;\ \varepsilon^2 Z, \varepsilon'^2 Z') = \Theta_Q(c, d;\ Z, Z')e_3,$$

$$(24d)\qquad \Theta_Q(c, d;\ -1/Z, -1/Z') = N(Z)^{n/2}\Theta_Q(d, c;\ Z, Z')e_4,$$

where the multipliers e_1, e_2, e_3, e_4 can be written as

$$(25a)\qquad e_1 = e[c^2\eta^2 q/4] = (w_1)^{c^2} \qquad \text{where} \qquad w_1 = e[\eta^2 q/4],$$

$$(25b)\qquad e_2 = e[c^2\eta^3 q/4] = (w_2)^{c^2} \qquad \text{where} \qquad w_2 = e[\eta^3 q/4],$$

$$(25c)\qquad e_3 = e[cdq\eta^2(\varepsilon-1)/2] = (w_3)^{cd} \qquad \text{where} \qquad w_3 = e[q\eta^2(\varepsilon-1)/2],$$

$$(25d)\qquad e_4 = e[cdq\eta^2/2] = (w_4)^{cd} \qquad \text{where} \qquad w_4 = e[q\eta^2/2],$$

and the sign of $N(Z)^{n/2}$ is defined (by analytic continuation) using the + sign when Z and Z' are purely imaginary.

For (24a), note that a change of Z to $Z+1$ augments the argument of $e[\dots]$ in (22) by the trinomial

$$Q(\Lambda+c\eta\Omega_t/2) = Q(\Lambda)+cQ(\Lambda, \eta\Omega_t)+c^2 q\eta^2/4.$$

The first of these terms is ignored since it lies in $\mathfrak{O}_2$; the second changes d to $d+c$ formally, while the third provides e_1.

For (24b) we note that changing Z to $Z+\eta$ effectively multiplies the augmenting trinomial (above) by η. Then, by Lemma 1, $\eta Q(\Lambda) \equiv Q(\Lambda, \eta\Omega_t) \pmod 2$ while $c\eta Q(\Lambda, \eta\Omega_t) \equiv 0 \pmod 2$, and $c^2 q\eta^3/4$ provides e_2.

Before proving (24c) we require the following:

LEMMA 3. *If we replace η by $\eta+2\gamma$ then the value of $\Theta_Q(c, d; Z, Z')$ changes by a "sign" factor (± 1) namely $e[cdq\gamma\eta]$, which depends only on the residue class of $\gamma \pmod{\mathfrak{O}_1}$.*

For proof merely change Λ to $\Lambda - c\gamma\Omega_t$ and η to $\eta+2\gamma$ in (22).

Then for (24c), we note that if Z is multiplied by ε^2 in (22) then ε^2 can be absorbed in $Q(\Lambda+c\eta\Omega_t/2)$ giving $Q(\varepsilon\Lambda+c\eta\varepsilon\Omega_t/2)$. This suggests that Λ is multiplied by ε which does not affect its generality while η is, however, also multiplied by ε. Likewise, since $1/\varepsilon = \pm\varepsilon' \equiv \varepsilon \pmod 2$, then $\varepsilon^2 \equiv 1$ and $dQ(\Lambda, \eta\Omega_t)$ can be replaced by $dQ(\varepsilon\Lambda, \varepsilon\eta\Omega_t)$ in (22). Thus the net effect of multiplying Z by ε^2 is to augment η by $\eta\varepsilon - \eta = 2(\varepsilon-1)\eta/2$, making Lemma 3 applicable with $\gamma = \eta(\varepsilon-1)/2$.

For the final result (24d) we extend the symbols Λ, Λ' and M, M', etc., to a pair of n-dimensional real vectors with functionally independent (nonalgebraic) components written $X = (x_1, \dots, x_n)$ and $X' = (x'_1, \dots, x'_n)$. We still keep the conventions in defining $e(\dots)$ analogously with (16ab), but we let $\int \dots dX$ denote the $2n$-fold integral from $-\infty$ to ∞ of $dx_1 \dots dx_n dx'_1 \dots dx'_n$.

LEMMA 4 (Poisson-Lipschitz). *If all sums encountered are absolutely convergent, then formally*

$$(26a)\qquad \sum_{\Lambda\in\mathfrak{O}^n} F(\Lambda, \Lambda') = \frac{1}{D^{n/2}} \sum_{M\in\mathfrak{O}^n} \int F(X, X')e\Big(-2\sum_{i=1}^{n} x_i\mu_i\Big)\,dX$$

where D is the discriminant of any nondegenerate quadratic module $\mathfrak{O}$.

The proof and necessary estimates are well established [1], [5], [8]. In our application we replace the variables μ_i by $\sum a_{ij}\mu_j$ which does not affect the generality of M in $\mathfrak{O}$ since the determinant of Q is a *unit* in $\mathfrak{O}$. Thus $\sum x_i\mu_i$ becomes $Q(X, M)$. If we now substitute

$$F(\Lambda, \Lambda') = e[ZQ(\Lambda+c\eta\Omega_t/2)+dQ(\Lambda, \eta\Omega_t)]$$

we obtain

$$(26b)\qquad \Theta_Q(c, d;\ Z, Z')$$

$$= \frac{1}{(4m)^{n/2}} \sum_{M\in\mathfrak{O}^n} \int e[ZQ(X+c\eta\Omega_t/2)+dQ(X, \eta\Omega_t)-2Q(X, M)]dX$$

which is the starting point for (24d).

To consummate the proof of (24d) we "complete the square in X" for the argument of $e[\dots]$ in (26b) obtaining

$$ZQ(X+c\eta\Omega_t/2+d\eta\Omega_t/2Z-M/Z)+Zc^2\eta^2 q/4-ZQ(c\eta\Omega_t/2+d\eta\Omega_t/2Z-M/Z).$$

The first term, being integrated by dX from $-\infty$ to ∞ is replaced by $ZQ(X)$ and it becomes removed from summation. The remaining two terms become

$$(-1/Z)Q(M-d\eta\Omega_t/2)+Q(c\eta\Omega_t,\ M-d\Omega_t\eta/2).$$

We can identify the "parts" of (24d) (replacing $-d$ by d) once we show

$$\int e[ZQ(X)]dX = D^{n/2}/N(Z)^{n/2},$$

but this follows from a (real) change of variables diagonalizing $Q(X)$ and $Q'(X')$ and permitting the integral to be decomposed in the fashion of the classical theta-function in one variable. Thus Lemma 2 is proved.

We now use Lemma 2 to find a way of defining four conjugate theta-functions independently of the choice of basis for Q. Certainly $\Theta_Q(0,0;Z,Z')$ is invariant, and by (24b) so is

$$\Theta_Q(0,1;Z,Z') = \Theta_Q(0,0;Z+\eta,Z'+\eta').$$

From (24d) we infer the invariance (under choice of basis for Q) of

$$\Theta_Q(1,0;Z,Z') = \Theta_Q(0,1;-1/Z,-1/Z')N(Z)^{-n/2}.$$

Finally, from (24b) again, we infer the invariance of

$$w_2\Theta_Q(1,1;Z,Z') = \Theta_Q(1,0;Z+\eta,Z'+\eta').$$

We can now define the invariant set of conjugate theta-functions belonging to a (classic) form Q with unit determinant representing only numbers in $\mathfrak{O}_2^+$ (or zero) as follows:

$$\theta_Q(c,d;Z,Z') = (w_2)^{c^2d^2}\Theta_Q(c,d;Z,Z'). \tag{27}$$

(Of course the factor $(w_2)^{c^2d^2}$ is w_2 if c and d are both odd, otherwise it is 1.)

We then verify

$$\theta_Q(c,d;Z+1,Z'+1) = \theta_Q(c,d+c;Z,Z')f_1, \tag{28a}$$

$$\theta_Q(c,d;Z+\eta,Z'+\eta') = \theta_Q(c,d+1;Z,Z')f_2, \tag{28b}$$

$$\theta_Q(c,d;\varepsilon^2Z,\varepsilon'^2Z') = \theta_Q(c,d;Z,Z')f_3, \tag{28c}$$

$$\theta_Q(c,d;-1/Z,-1/Z') = N(Z)^{n/2}\theta_Q(d,c;Z,Z')f_4, \tag{28d}$$

where the new multipliers are given in terms of the w_i in (25) as

$$f_1 = [w_1w_2^{2d-1}]^{c^2}, \quad f_2 = w_2^{2dc^2}, \quad f_3 = w_3^{cd}, \quad f_4 = w_4^{cd}. \tag{29}$$

LEMMA 5. *The multipliers* (29) *are all* 1 *if and only if q lies in* $2\mathfrak{O}_2$.

For the proof of Lemma 5, observe that for all f_i to equal 1 (regardless of c and d) it is necessary and sufficient that w_1w_2, w_2^2, w_3, and w_4 all equal 1. From $w_2^2 = w_4 = 1$, it follows that $e[(q\eta^2/2)\lambda] = 1$ for arbitrary λ in $\mathfrak{O}$ (and conversely); thus $w_2^2 = w_4 = 1$ precisely when $q \equiv 0 \pmod 2$. The fact that $w_3 = 1$ then contributes nothing further. We set $q = 2k$

and ask when $w_1w_2 = e[\eta^2(1+\eta)k/2] = 1$? Since $\eta^2(1+\eta)/2 \equiv 1 \pmod 2$, it is seen that the question is answered positively precisely when k lies in $\mathfrak{O}_2$, proving Lemma 5.

We shall also need to consider the symmetry operation of interchanging Z, Z' with $-Z', -Z$ (which preserves the half-planes (16a)).

LEMMA 6. *If Q' denotes the conjugate of Q, the*

$$\theta_Q(c,d;-Z',-Z) = \theta_{Q'}(c,d;Z,Z')e(q\eta cd\sqrt{m}).$$

For proof, we verify that

$$\Theta_Q(c,d;-Z',-Z) = \sum_{\Lambda\in\mathfrak{O}^n} e[ZQ'(\Lambda'+c\eta'\Omega_t/2) - dQ'(\Lambda',\eta'\Omega_t)]$$

summed over Λ' which is also arbitrary in $\mathfrak{O}^n$. Thus the net effect is precisely the same as replacing η by $\eta' = \eta - 2\sqrt{m}$; and we can apply Lemma 3 with $\gamma = -\sqrt{m}$ and $q' \equiv q \pmod 2$.

In the cases (15) we note that all of the forms cited are equivalent to their conjugates under an easy sign-permutation. Hence $\theta_Q = \theta_{Q'}$. Generally, when Q and Q' are equivalent, the conjugate operation does not affect θ_Q unless m and q are both odd; then it becomes a question of the factor $(-1)^{cd}$.

We might conclude this section by noting first that θ_Q is not independent of the choice of η (belonging to $\mathbf{2}_1$ but not to $\mathbf{2}_1^2$). If we replace η by $\eta+2\gamma$, then a possible sign-change $e[qcd\gamma\eta^2/2]$ is introduced into θ_Q. Moreover we note that the functions Θ_Q or θ_Q are never identically zero, since when $c = d = 0$, $\Theta_Q = 1$ at $Y = -Y' = \infty$ while the other values of c and d are connected by the functional equations. Of special interest is the fact that *the four conjugates are identically the same if and only if Q is an even form*. If Q is even, it is simple to verify that $q = t = 0$; while the converse is established by expanding the first few terms (but the details can be omitted as this converse result is not needed).

4. Main theorem and applications. Collecting all our previous results we find we have proved the following:

MAIN THEOREM. *Let Q be a (classic) n-ary quadratic form with unit determinant and coefficients in $\mathfrak{O}$ representing only numbers in $\mathfrak{O}_2^+$ (and zero). Let a value q be determined as in* (13) *by its semidiagonalized form. Consider the invariant set of conjugate theta-functions*

$$\theta_Q(c,d;Z,Z') = \sum_{\Lambda\in\mathfrak{O}^n} e[ZQ(\Lambda+c\eta\Omega_t/2) + dQ(\Lambda,\eta\Omega_t) + c^2d^2\eta^3q/4]. \tag{31}$$

Then the functional equations (28a-d) *for the generators* (21) *of $\mathfrak{G}^*$ will have constants f_1, f_2, f_3, f_4 determined by c and d and precisely by the value of q modulo $2\mathfrak{O}_2$.*

The most immediate application is that we have a transcendental proof of the invariance of q modulo $2\mathfrak{O}_2$ under change of basis of Q! Furthermore, the value of q modulo $2\mathfrak{O}_2$ is effectively the "genus invariant" that makes the functional equations (28a-d) valid.

A. *The Forms in* $Q(\sqrt{3})$. Turning our attention to the forms Q_0, Q_1, Q_2, Q_3 for $Q(\sqrt{3})$, we see all values of q in (15) are congruent modulo $2\mathfrak{O}_2$ and the theta-functions are symmetric (see Lemma 6). Now it was seen in [2], § 32, that the holomorphic solutions of the functional equations (28a-d) with all $f_i = 1$ and $n = 4$ form a vector space of dimension 3 over the complex numbers. The Eisenstein series

$$1 + \sum_{\mu \in \mathfrak{O}_2^+}{}' B(\mu) e(\mu Z), \qquad 1 + \sum_{\mu \in \mathfrak{O}_2^+}{}' 24 D(\mu) e(\mu Z)$$

are already known ([1],[2]); hence these functions together with the "unknown" $[\Theta^{(1)}]^4$ (see (19b)) constitute a basis. A check of the first few coefficients yields the representation theorems (1b), (4b), (5b), and (6b) as required.

B. *Reduction to modular identities in one variable.* While we do not repeat the proof of the basis theorem just cited, we recall that the Siegel-Götzky technique avoided the genus argument by working directly with a one-(complex)-dimensional submanifold of the bicomplex space (16a). Many unusual number theoretic identities emerge if we do this ([1], § 9, [3], § 42).

To see this possibility in the simplest light, let us henceforth restrict Q to be Q_0, an even form, so all four theta-functions coincide:

$$\theta_{Q_0}(Z, Z') = \sum_{A \in \mathfrak{O}^n}{}' e[ZQ(A)] = 1 + \sum_{\mu \in 2\mathfrak{O}^+}{}' R_0(\mu) e(\mu Z). \tag{33}$$

Here, as usual, $R_0(\mu)$ is the number of representations of $Q_0 = \mu$ (for μ in $2\mathfrak{O}^+$).

We next define two modular forms in one complex variable U in the half-plane $\operatorname{Im} U = 0$, namely

$$\psi(U) = \theta_{Q_0}(U, -U) \tag{34a}$$

and, when $N(\varepsilon) = -1$ or $\varepsilon > 0 > \varepsilon'$ we define

$$\varphi(U) = \theta_{Q_0}(\varepsilon U, \varepsilon' U). \tag{35a}$$

Then by specializing the appropriate equations from the set (28a-d) we find $\psi(U)$ and $\varphi(U)$ satisfy identities of the type

$$\Phi(U+\xi) = \Phi(U), \quad \Phi(-1/U) = U^n i^n \Phi(U); \tag{36}$$

specifically,

$$\psi(U) = \Phi(U) \quad \text{for} \quad \xi = \sqrt{m}, \tag{37a}$$

$$\varphi(U) = \Phi(U) \quad \text{for} \quad \xi = 1. \tag{37b}$$

Now there are certain well-known ([4], [6]) solutions to (36) by Eisenstein series in special cases. Let us define for n even

$$G_n(U) = 1 - \frac{2n}{B_n} \sum_{r=1}^{\infty} \exp 2\pi i U \cdot \sigma_{n-1}(r), \tag{38}$$

where $\sigma_s(r)$ is the sum of the s-powers of the divisors of r (referring to positive rational integers), and B_n represents the Bernoulli numbers ($B_2 = 1/6$, $B_4 = -1/30$, $B_6 = 1/42, \ldots$). *Then if* $4|n$, *we find that* $G_n(U)$ *satisfies* (36) *for* $\xi = 1$.

From $G_n(U)$ we can construct, for n even,

$$H_n(U) = [G_n(U/\sqrt{m}) + (-m)^{n/2} G_n(U\sqrt{m})]/[1 + (-m)^{n/2}], \tag{39}$$

(normalized, like $G_n(U)$, so that $H_n(\infty) = 1$). *Then if* n *is even* $H_n(U)$ *satisfies* (36) *for* $\xi = \sqrt{m}$.

Assuming that Φ is holomorphic and bounded at ∞, there exists a well-known procedure (due to Poincaré) for constructing the most general solution to (36) in terms of the Klein or Hecke Invariant $I(U)$ (corresponding to $n = 0$ in (36)), which maps the fundamental domain onto the I-sphere. The details are quite standard ([1], § 8) but we shall quote only the simplest type of result for the present:

LEMMA 7. *Consider solutions to the functional equation* (36) *which are holomorphic and bounded at* ∞.

If $\xi = 1$ *and* $n = 4$ *or* 8 *all such solutions are proportional to a single solution, necessarily* $G_n(U)$ *(and indeed* $G_8 = G_4^2$*).*

If $\xi = \sqrt{2}$ *and* $n = 2, 4$, *or* 6 *all such solutions are proportional to a single solution, necessarily* $H_n(U)$ *(and indeed* $H_4 = H_2^2$, $H_6 = H_2^3$*).*

If $\xi = \sqrt{3}$ *and* $n = 2$ *or* 4 *all such solutions are proportional to a single solution, necessarily* $H_n(U)$ *(and indeed* $H_4 = H_3^2$*).*

C. *Divisor identities.* Obviously, Lemma 7 leads very naturally to identities. We can rewrite (34a) and (35a) as

$$\psi(U) = 1 + \sum_{a=1}^{\infty} r(a) \exp 2\pi i a U/\sqrt{m}, \tag{40a}$$

$$\varphi(U) = 1 + \sum_{b=1}^{\infty} s(b) \exp 2\pi i b U, \tag{41a}$$

where

(40b) $$r(a) = \sum_{b=-a\sqrt{m}}^{a\sqrt{m}} R_0(2a+2b\sqrt{m}),$$

(41b) $$s(b) = \sum_{a=-b\sqrt{m}}^{b\sqrt{m}} R_0\big((2a+2b\sqrt{m})\varepsilon\big) \quad (N(\varepsilon) = -1),$$

summing, of course, only over integral values of b or a.

It will then follow that for the values specified in Lemma 7, $r(a)$ and $s(b)$ are related to the divisor functions σ_{n-1} by (39) and (38) as follows:

(40c) $$r(a) = -\left(\frac{2n}{B_n}\right)\frac{\sigma_{n-1}(a)+(-m)^{n/2}\sigma_{n-1}(a/m)}{1+(-m)^{n/2}},$$

(41c) $$s(b) = -\frac{2n}{B_n}\sigma_{n-1}(b),$$

where $\sigma_{n-1}(\dots)$ *is interpreted as zero for nonintegral argument.*

It is still required that an even form Q_0 *exist* to make the identities (40c) and (41c) realizeable! There is a rather elaborate arithmetic theory on the existence of even forms ([11], [9]) into which it is not necessary to enter. We merely note that for various values of m with $N(\varepsilon) = -1$ it may well happen that there are many even forms Q_0; nevertheless for each of these Q_0 (possibly with different R_0-functions) the $s(b)$-function will be always given by (41c) for $n = 4, 8$.

When $m = 2$ an even form coming under Lemma 7 (for $n = 4$) is

(42a) $$Q_0 = 2(\xi_1^2+\xi_1\xi_2+\xi_2^2+\xi_3^2+\xi_3\xi_4+\xi_4^2)+2\sqrt{2}\,(\xi_1\xi_4+\xi_4\xi_2+\xi_2\xi_3).$$

For this function, from the methods of [1], it follows that $R_0(\mu) = 48D(\mu/2)$; hence (41c) becomes

(42b) $$\sum_{a=-b\sqrt{2}}^{b\sqrt{2}} D(a+b\sqrt{2}) = 5\sigma_3(b).$$

(Of course, here we have adapted the D-function of (2) to refer to $Q(\sqrt{2})$, where $\varepsilon = 1+\sqrt{2}$.) On the other hand, (40c) becomes

(42c) $$\sum_{b=-a/\sqrt{2}}^{a/\sqrt{2}} D(a+b\sqrt{2}) = \sigma_3(a)+4\sigma_3(a/2).$$

When $m = 3$, we have an even form ($n = 2$), namely

(43a) $$Q_*(\xi_1, \xi_2) = 2\xi_1^2+2\sqrt{3}\,\xi_1\xi_2+2\xi_2^2,$$

hence for $n = 2t$ we have for the vector $\Xi = (\xi_1, \dots, \xi_n)$

(43b) $$Q_0(\Xi) = Q_*(\xi_1, \xi_2)+\dots+Q_*(\xi_{n-1}, \xi_n).$$

For $n = 4$, by (6b), $R_0(\mu) = 24D(\mu/2)$ and

(43c) $$\sum_{b=-a/\sqrt{3}}^{a/\sqrt{3}} D(a+b\sqrt{3}) = \sigma_3(a)+9\sigma_3(a/3).$$

(There is of course no analogue of (42b) since $N(\varepsilon) = 1$.)

When $m = 5$, the theta-function presents a more complicated situation ([5]) as there are *ten* conjugates (not four). The data for the corresponding result for $n = 4$ can be extracted, however, from Maass' work [8]. There the following even form was displayed:

(44a) $$Q_0 = 2(\xi_1^2+\xi_2^2+\xi_3^2-\xi_3\xi_4+\xi_4^2)+2\varepsilon(\xi_1\xi_3+\xi_2\xi_4)+2\varepsilon'(\xi_1\xi_4+\xi_2\xi_3),$$

where $\varepsilon = (1+\sqrt{5})/2$, and it was shown that $R_0(\mu) = 120D(\mu)$. Hence our methods yield the following identity:

(44b) $$\sum_{a=-b\sqrt{5}}^{b\sqrt{5}} D\left(\frac{a+b\sqrt{5}}{2}\right) = 2\sigma_3(b)$$

(where the summation is restricted to $a \equiv b \pmod 2$ of course). The details of (44b) are omitted since they come under a different formalism.

D. *Rational results.* The summation functions $r(a)$ and $s(b)$ actually can be interpreted as "rational" functions. To take the simpler case, we see

(45a) $r(a)$ = number of representations of $Q_0 = 2(a+b\sqrt{m})$ with a prescribed and b unspecified,

or, if we write $Q_0 = Q_0^{(R)}+\sqrt{m}\,Q_0^{(I)}$ in terms of a "rational" and an "irrational part", then

(45b) $r(a)$ = number of representations of $Q_0^{(R)} = 2a$.

Only one case really works out elegantly. Take $Q_*(\xi_1, \xi_2)$ in (43a) and note that if $\xi_1 = x_1-x_2+x_4\sqrt{3}$, $\xi_2 = x_3-x_4+x_2\sqrt{3}$; then the rational part of Q_* is $2Q^*(x_1, x_2)+2Q^*(x_3, x_4)$ where Q^* is the (nonclassic) form

(46) $$Q^*(x_1, x_2) = x_1^2+x_1x_2+x_2^2.$$

Thus the rational part of $Q_0(\Xi)$ in (43b) becomes (for $n = 2t$)

(47a) $$Q^{(t)} = Q^*(x_1, x_2)+\dots+Q^*(x_{4t-1}, x_{4t});$$

and $r(a)$ for (43b) becomes (say) $r_t(a)$, *the number of representations of* $Q^{(t)} = a$ *in terms of the* $4t$*-tuples of rational integers* $(x_1, \ldots, x_{4t})$. It is given by

$$r_t(a) = -\left(\frac{4t}{B_{2t}}\right) \cdot \frac{\sigma_{2t-1}^{(a)} + (-3)^t \sigma_{2t-1}^{(a/3)}}{1+(-3)^t} \tag{47b}$$

for $t = 1$ and 2, according to Lemma 7.

In the case of $\sqrt{2}$ and $\sqrt{5}$ the rational octenary forms corresponding to (47a) are too complicated for the identity of type (40c) or (41c) to be worth explicit formulation. Of course these rational forms (unlike the algebraic forms) have nonunit determinant.

In order to present the simplest type of identities we ignored some very interesting noneven cases such as the "sum of four squares" in $Q(\sqrt{2})$ and $Q(\sqrt{3})$ where the theta-functions $\theta_Q(1, 1; U, -U)$ and $\theta_Q(1, 1; \varepsilon U, \varepsilon' U)$ satisfy the system (36). A partial treatment of these cases appears in [1], [2] but a more thorough treatment of identities, indeed a treatment embracing a larger number of field types, must wait for a later occasion.

References

[1] H. Cohn, *Decomposition into four integral squares in the fields of* $2^{1/2}$ *and* $3^{1/2}$, Amer. J. Math. 82 (1960), pp. 301-322.

[2] — *Cusp forms arising from Hilbert's modular functions for the field of* $3^{1/2}$, Amer. J. Math. 84 (1962), pp. 283-305.

[3] — and G. Pall, *Sum of four squares in a quadratic ring*, Trans. Amer. Math. Soc. 105 (1962), pp. 536-556.

[4] R. Fueter, *Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen*, Leipzig 1924.

[5] F. Götzky, *Über eine zahlentheoretische Anwendung von Modulfunktionen zweier Veränderlichen*, Math. Ann. 100 (1928), pp. 411-437.

[6] E. Hecke, *Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichungen*, Math. Ann. 112 (1936), pp. 664-699.

[7] B. W. Jones, *The arithmetic theory of quadratic forms*, New York 1950.

[8] H. Maass, *Modulformen und quadratische Formen über dem quadratischen Zahlkörper* $R(\sqrt{5})$, Math. Ann. 118 (1941), pp. 65-84.

[9] — *Quadratische Formen über quadratischen Körpern*, Math. Zeit. 51 (1945), pp. 233-254.

[10] L. J. Mordell, *On Mr. Ramanujan's Empirical Expansions of Modular Functions*, Proc. Cambridge Phil. Soc. 19 (1917), pp. 117-124.

[11] — *The definite quadratic forms in eight variables with determinant unity*, Journal de Mathematiques pures et appliquées 17 (1938), pp. 11-46.

[12] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*, Ann. of Math. 36(1935), pp. 527-606; 37(1936), pp. 230-263; 38(1937), pp. 212-291.

UNIVERSITY OF ARIZONA, TUCSON, U. S. A.

Reçu par la Rédaction le 30. 5. 1963

ACTA ARITHMETICA
IX (1964)

Functions and polynomials $(\mathrm{mod}\, p^n)$*

by

L. Carlitz (Durham, North Carolina)

To Professor L. J. Mordell on his seventy-fifth birthday

1. Let p be a fixed prime and n an integer $\geqslant 1$. Let Z_n denote the ring of integers $(\mathrm{mod}\, p^n)$. By a *function* f over Z_n will be meant a mapping of Z_n into itself; that is, $f(a) \in Z_n$ for all $a \in Z_n$. Two functions f, g over Z_n are *equal* provided

$$f(a) \equiv g(a) (\mathrm{mod}\, p^n)$$

for all $a \in Z_n$.

A *polynomial* $F(x)$ is a function of the type

$$F(x) = a_0 + a_1 x + a_2 x^2 + \ldots \qquad (a_j \in Z_n). \tag{1}$$

When $n = 1$ it is well known that every function over Z_n can be represented as a polynomial. When $n > 1$, however, this is no longer true. For example, the function defined by

$$f(a) = \begin{cases} 0 & (a = 0), \\ 1 & (a \neq 0) \end{cases} \tag{2}$$

cannot be represented as a polynomial. This follows from the observation that for any polynomial $F(x)$ we have

$$F(a+p) \equiv F(a) (\mathrm{mod}\, p); \tag{3}$$

clearly (2) and (3) are not compatible.

The representation (1) is, of course, not unique. When $n = 1$ the representation is unique provided $\deg F(x) < p$. When $n \geqslant 1$, let $F(x)$, $G(x)$ be two polynomials such that

$$F(a) \equiv G(a) (\mathrm{mod}\, p^n) \tag{4}$$

* Supported in part by National Science Foundation grant G16485.