где $\vartheta_j(\tau)$ — якобиевы тэта-функции; $\varrho_{2k}(n)$ — сумма сингулярного ряда Харди, отвечающего сумме $2k$ квадратов целых чисел; $\alpha_{2k}^{(t)}$ — постоянные, подобранные надлежащим образом; $l = \left[\frac{2k-1}{8}\right]$. Приравнивая коэффициенты при $e^{\pi i\tau n}$ в обеих частях этого тождества, получаем формулы для $r_{2k}(n)$, выписанные выше.

Мы предполагаем, что функциональным эквивалентом формул для арифметической функции $r(n, F_k)$ будет тождество

$$(*) \qquad \vartheta(\tau, F_k) = E(\tau, F_k) + \sum_{t=1}^{l} \alpha_k^{(t)} \vartheta(\tau, F_{k-2-2t}, \varphi_{2+2t}^{(k-2-2t)}),$$

где $l = \sum_{m=1}^{\infty} \left[\frac{k}{6m}\right]$; $\alpha_k^{(t)}$— постоянные, которые следует подбирать надлежащим образом. Это действительно так при $2 \leqslant k \leqslant 17$, ибо доказанные выше тождества (1.11), (4.4), (4.6), (4.8), (4.14), (4.20), (4.26), (5.8), (5.9), (5.10), (5.16), (5.17), и (5.18) являются частными случаями тождества (*). А в настоящей работе показано, что формулы для $r(n, F_k)$ следуют из упомянутых тождеств приравниванием в их обеих частях коэффициентов при z^n. Желательно доказать, что тождество (*) имеет место при всех $k \geqslant 2$ или опровергнуть это предположение.

Литература

[1] V. Boulyguine, *Sur une application des fonctions elliptiques au problème de représentation des nombres entiers par une somme de carrés*, Изв. Императорской Академии Наук, Сер. 6, № 6 (1914), 389-404.

[2] Л. Е. Диксон, *Введение в теорию чисел*, Обработанный перевод с английского А. З. Вальфиша, Тбилиси 1941.

[3] E. Hecke, *Mathematische Werke*, Zweite Auflage, Göttingen 1970.

[4] Г. А. Ломадзе, *О представлении чисел суммами квадратов*, Тр. Тбилис. матем. ин-та им. А. М. Размадзе, 16 (1948), 231–275.

[5] —*К представлению чисел суммами квадратов*, Тр. Тбилис. матем. ин-та им. А. М. Размадзе, 20 (1954), 47-87.

[6] —*О параболических формах простой ступени и главного типа*, Тр. Тбилис. матем. ин-та им. А. М. Размадзе, 57 (1977), 63–81.

[7] — *О представлении чисел суммами квадратичных форм* $x_1^2 + x_1x_2 + x_2^2$, Тезисы докл. Всесоюзной конференции „Теория чисел и ее приложения" (17–19 сентября 1985 г., Тбилиси), с. 140.

[8] L. J. Mordell, *On the representations of numbers as a sum of 2r squares*, Quart. J. Pure Appl. Math. 48 (1917), 93–104.

[9] H. Petersson, *Modulfunktionen und quadratische Formen*, Berlin-Heidelberg-New York 1982.

[10] A. Walfisz, *Zur additiven Zahlentheorie*, Тр. Тбилис. матем. ин-та 5 (1938), 69–114.

Поступило 21.5.1987 (1725)

ACTA ARITHMETICA
LIV (1989)

Selberg zeta functions with virtual characters and the class number

by

JEFFREY STOPPLE (Santa Barbara, Cal.)

1. Introduction. In [3], Hecke investigated the action of the modular group in spaces of holomorphic forms for principal congruence subgroups $\Gamma(q)$. For forms of weight 2, he obtained the complete decomposition of the representation into irreducible components. He also proved the curious fact that the difference of the multiplicities of two particular representations was equal the class number of the imaginary quadratic field $\boldsymbol{Q}(\sqrt{-q})$. Later Feldman [1] studied arbitrary weight, Saito [7] studied Hilbert modular forms, and Hashimoto, in [2] considered Siegel modular forms. Each found similar class number formulas.

The group SL(2, $\boldsymbol{Z}$) also acts by linear fractional transformation in the vector space of Maass cusp forms for $\Gamma(q)$. Since $\Gamma(q)$ acts trivially the representation is equivalent to one of the factor group SL(2, $\boldsymbol{F}_q$). This paper will prove a formula analogous to Hecke's relating multiplicities of representations π^+ and π^- in these spaces to the class number and fundamental unit of the real quadratic field $\boldsymbol{Q}(\sqrt{q})$. (The representations π^+ and π^- are defined below.) Of course, Maass cusp forms are themselves very intractible objects, so no new results on class numbers are to be expected.

For convenience we will study the zeros of the quotient of Selberg zeta functions $Z(s, \pi^+)/Z(s, \pi^-)$, which is equivalent to the problem described above for Maass cusp forms.

We need some definitions. Let q be a prime, $q \equiv 1(4)$. We can define a character χ on the upper triangular subgroup of SL(2, $\boldsymbol{F}_q$) by

$$\chi \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix} = \left(\frac{a}{q}\right)$$

for $\left(\frac{a}{q}\right)$ the Legendre symbol. We can form the corresponding induced representation of SL(2, $\boldsymbol{F}_q$), which has two irreducible components:

$$\mathrm{ind}(\chi) \cong \pi^+ \oplus \pi^-.$$

Let ψ be a virtual character of the group defined by

$$\psi(g) = \operatorname{trace} \pi^+(g) - \operatorname{trace} \pi^-(g).$$

From tables [11] we see that

$$\psi(g) = \begin{cases} \sqrt{q}\left(\dfrac{x}{q}\right) & \text{if } g \in SL(2, F_q) \text{ is conjugate to a matrix } \pm\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}, \\ 0 & \text{otherwise.} \end{cases}$$

2. The functional equation. The Selberg zeta function is defined by

$$Z(s, \varrho) = \prod_{\{P\}} \prod_{k=0}^{\infty} \det(I - \varrho(P) N(P)^{-s-k}).$$

Here ϱ is any finite dimensional representation of $SL(2, \mathbf{Z})$, $\{P\}$ is a primitive hyperbolic conjugacy class in $SL(2, \mathbf{Z})$, and $N(P)$ is ε^2, where ε is the larger eigenvalue of P. The logarithmic derivative of $Z(s, \varrho)$ is given by the trace formula. There is also a functional equation involving contributions from the central, elliptic and parabolic classes, as well as from the continuous spectrum of the trace formula. More details on this function can be found in [4] and [9]. In particular, if ϱ is a representation of SL $(2, F_q)$, it is known (see [5], [10]) that the multiplicity of a zero s_0 of $Z(s, \varrho)$ is equal to the multiplicity of ϱ for the action of $SL(2, \mathbf{Z})$ in the vector space of Maass cusp forms for eigenvalue $s_0(1 - s_0)$ and level q.

We will prove a theorem about the difference of the multiplicities of the two representations π^+ and π^- by considering the quotient of Selberg zeta functions

$$Z(s, \psi) = \frac{Z(s, \pi^+)}{Z(s, \pi^-)}.$$

From [10] we know that π^+ and π^- are both $(q+1)/2$ dimensional, and each gives a single continuous spectrum as representations of $SL(2, \mathbf{Z})$; i.e., $c_{\pi^+} = c_{\pi^-} = 1$ in the notation of [10]. The corresponding scattering matrices are

$$\Phi(s, \pi^{\pm}) = \pm\left(\frac{\pi}{q}\right)^{2s-1} \frac{\Gamma(1-s)}{\Gamma(s)} \frac{L\left(2-2s, \left(\dfrac{*}{q}\right)\right)}{L\left(2s, \left(\dfrac{*}{q}\right)\right)}.$$

Thus $Z(s, \pi^+)$ and $Z(s, \pi^-)$ have the same contributions in their functional equation from the central term and the continuous spectrum term. The elliptic terms are also equal, as $|\operatorname{trace}(\gamma)| < 2 \Rightarrow \operatorname{trace}(\gamma) \not\equiv \pm 2(q)$ so $\psi(\gamma) = 0$ for γ elliptic in $SL(2, \mathbf{Z})$.

All that remains is the parabolic classes contribution to the discrete spectrum. Suppose $\pi^+\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has eigenvalues $\{\ldots, e^{2\pi i \alpha_j^+}, \ldots\}$ and $\pi^-\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has eigenvalues $\{\ldots, e^{2\pi i \alpha_j^-}, \ldots\}$. Then

$$Z(1-s, \psi) = Z(s, \psi) \exp\{(1-2s)\Big(\sum_{\alpha_j^+ \neq 0} \log|1 - e^{2\pi i \alpha_j^+}| - \sum_{\alpha_j^- \neq 0} \log|1 - e^{2\pi i \alpha_j^-}|\Big)\}.$$

From [10] we know the eigenvalues of $\pi^{\pm}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ are all nontrivial q roots of 1 corresponding to squares and nonsquares respectively in F_q^*. Since $|1 - e^{2\pi i a/q}| = 2\sin(\pi a/q)$ we see that

$$Z(1-s, \psi) = Z(s, \psi) \exp\left\{(1-2s) \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \log|\sin \pi a/q|\right\}.$$

By the Dirichlet class number formula,

$$Z(1-s, \psi) = Z(s, \psi)\, \varepsilon^{2h(2s-1)}$$

where h is the narrow class number, and ε the fundamental positive norm unit in $\mathbf{Q}(\sqrt{q})$.

3. The trace formula. We now consider the logarithmic derivative

$$\frac{Z'}{Z}(s, \psi) = \sum_{\{P\}} \sum_{k=1}^{\infty} \frac{\psi(P^k) \log NP}{NP^{k/2} - NP^{-k/2}} \frac{1}{NP^{s-1/2}}. \tag{3.1}$$

Define a map φ from matrices P to quadratic forms by

$$\varphi\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \left[\frac{b}{v}, \frac{d-a}{a}, \frac{-c}{v}\right]$$

where $v = \gcd(b, d-a, c)$. Conversely a form $[\alpha, \beta, \gamma]$ with discriminant $D = \beta^2 - 4\alpha\gamma$ is mapped to

$$P = \begin{bmatrix} \dfrac{t - u\beta}{2} & u\alpha \\ -u\gamma & \dfrac{t + \beta u}{2} \end{bmatrix}$$

where $t^2 - u^2 D = 4$ is the fundamental solution of Pell's equation. Note that NP is the larger root of $x^2 - tx + 1$, and thus depends only on the discriminant.

Sarnak [8] shows that φ is a 2-1 map (since $\varphi(P) = \varphi(-P^{-1})$) and φ commutes with the action of the modular group giving a 2-1 correspondence between primitive hyperbolic conjugacy classes $\{P\}$ and equivalence classes of quadratic forms.

Suppose P corresponds to $[\alpha, \beta, \gamma]$ with discriminant D and $t^2-Du^2=4$ fundamental solution. From the definition of ψ in Section 1 it is easy to see that

$$\psi(P^k)=\begin{cases}\left(\dfrac{ku\alpha}{q}\right)\sqrt{q} & \text{if} \quad q|D,\\ 0 & \text{if} \quad q\nmid D.\end{cases}$$

Thus we have (3.1) reduces to

$$2\sqrt{q}\sum_{\substack{D\\ q|D}}\ \sum_{\substack{\text{classes}\\ [\alpha,\beta,\gamma]\\ \text{with disc.}D}}\ \sum_{k=1}^{\infty}\left(\frac{ku\alpha}{q}\right)(NP\ \text{terms}) \tag{3.2}$$

$$=2\sqrt{q}\sum_{\substack{D\\ q|D}}\sum_{k=1}^{\infty}\left(\frac{ku}{q}\right)(NP\ \text{terms})\sum_{\substack{\text{classes}\\ [\alpha,\beta,\gamma]}}\left(\frac{\alpha}{q}\right).$$

Now $\left(\frac{\alpha}{q}\right)$ is multiplicative on classes of forms since the composition law is

$$[\alpha, \beta, *]\circ[\alpha', \beta, *]=[\alpha\alpha', \beta, *].$$

If $D=qd^2$ then we have $qd^2\equiv\beta^2 \bmod 4\alpha$ so $\left(\frac{\alpha}{q}\right)=\left(\frac{q}{\alpha}\right)=1$ for all classes (recall $q\equiv 1\,(4)$). Similarly if $D=qnd^2$ with n square free, we see the character is non-trivial. Thus by orthogonality the inner sum is 0 unless $D=qd^2$.

Let $\varepsilon_d=(t+u\sqrt{qd^2})/2$ be the unit $\mathbf{Q}(\sqrt{q})$ corresponding to the Pell solution $t^2-u^2qd^2=4$, and let $h(qd^2)$ be the class number of forms. We now have (3.2) equals

$$4\sqrt{q}\sum_{d=1}^{\infty}h(qd^2)\log\varepsilon_d\sum_{k=1}^{\infty}\frac{\left(\frac{ku}{q}\right)}{\varepsilon_d^k-\varepsilon_d^{-k}}\varepsilon_d^{k(1-2s)}. \tag{3.3}$$

From Lang [6] we know

$$h(qd^2)=\frac{hd}{[0^*:\mathbf{Z}[\varepsilon_d]^*]}\prod_{p|d}\left(1-\left(\frac{p}{q}\right)\frac{1}{p}\right)$$

and

$$\log\varepsilon_d=[0^*:\mathbf{Z}[\varepsilon_d]^*]\log\varepsilon,$$

where h and ε are the narrow class number, and fundamental positive norm unit in $\mathbf{Q}(\sqrt{q})$. Thus

$$\frac{Z'}{Z}(s,\psi)=4h\log\varepsilon\sqrt{q}\sum_{d=1}^{\infty}d\prod_{p|d}\left(1-\left(\frac{p}{q}\right)\frac{1}{p}\right)\sum_{k=1}^{\infty}\frac{\left(\frac{kv}{q}\right)\varepsilon_d^{k(1-2s)}}{\varepsilon_d^k-\varepsilon_d^{-k}}. \tag{3.4}$$

We want to group all terms of the form $\varepsilon_d^k=\varepsilon^n$ for $n=1, 2, \dots$, so write

$$\varepsilon^n=\frac{t(n)+f(n)\sqrt{q}}{2},\qquad \varepsilon_d=\frac{t+u\sqrt{qd^2}}{2}=\frac{t_d+u_d\sqrt{qd^2}}{2} \tag{$*$}$$

(i.e. we keep track of the dependence on n and d). Then

$$\varepsilon_d^k=\frac{\text{some integer}+\Big[\sum\limits_{\substack{j=1\\ \text{odd}}}^{k}\binom{k}{j}t_d^{k-j}u_d^jd^jq^{(j-1)/2}\Big]\sqrt{q}}{2^k}. \tag{$**$}$$

Since $t_d\equiv\pm 2(q)$ equating $(*)$ and $(**)$ gives

$$\left(\frac{ku_d}{q}\right)=\left(\frac{f(n)/d}{q}\right).$$

Also $\varepsilon_d^k-\varepsilon_d^{-k}=f(n)\sqrt{q}$ so we get (3.4) equals

$$4h\log\varepsilon\sum_{n=1}^{\infty}\left\{\sum_{d|f(n)}\left(\frac{f(n)/d}{q}\right)\frac{d}{f(n)}\prod_{p|d}\left(1-\left(\frac{p}{q}\right)\frac{1}{p}\right)\right\}\varepsilon^{n(1-2s)}. \tag{3.5}$$

One can expand the product term and use facts about the Möbius function to see that the term in braces is equal to 1. Thus

$$\frac{Z'}{Z}(s,\psi)=4h\log\varepsilon\sum_{n=1}^{\infty}\varepsilon^{n(1-2s)}=4h\log\varepsilon\left(\frac{\varepsilon^{1-2s}}{1-\varepsilon^{1-2s}}\right)$$

and we have proved the following

THEOREM. *For ψ as in Section* 1,

$$Z(s,\psi)=(1-\varepsilon^{1-2s})^{2h}.$$

(The fact that $Z(s,\pi^+)$ and $Z(s,\pi^-)$ both tend to 1 as $s\to\infty$ gives the constant of integration.) This theorem actually implies the functional equation we proved in Section 2.

Notice that $Z(s,\psi)$ has zeros at $s=\frac{1}{2}+k\pi i/\log\varepsilon$ for $k\in\mathbf{Z}$ with multiplicity $2h$. It is already known that $Z(s,\pi^+)$ and $Z(s,\pi^-)$ each have zeros at these points, corresponding to the cusp forms constructed by Maass. These cusp forms have Mellin transforms as Hecke L-functions attached to grossencharacters for the real quadratic field. Since these cusp forms transform under $\Gamma_0(q)$ according to the character $\left(\frac{*}{q}\right)$, the Frobenius reciprocity theorem implies they transform under $\mathrm{SL}(2, \mathbf{Z})$ according to either π^+ or π^-.

According to Langland's philosophy, the sum of the multiplicities of the zeros for $Z(s,\pi^+)$ and $Z(s,\pi^-)$ at these points should be the number of L functions attached to two dimensional representations (of Weil groups) with conductor q and determinant character $\left(\frac{*}{q}\right)$. The fact that the difference of the multiplicities of the zeros equals $2h$ is the exact analog for Maass wave forms of the theorem of Hecke for holomorphic forms mentioned in the introduction. This follows from the result about zeros of Selberg zeta functions mentioned at the beginning of Section 2.

The theorem also gives the surprising result that all other zeros of $Z(s, \pi^+)$ and $Z(s, \pi^-)$ are equal and occur with the same multiplicity. The author has no explanations for this.

References

[1] H. Feldmann, *Über das Verhalten der Modulfunktionen von Primazahlstufe bei beliebigen Modulsubstitution*, Abh. Math. Seminar der Hamburg Univ. 8 (1931), 323–347.

[2] K. Hashimoto, *Representations of the Finite Symplectic Group* SP (4, F_p) in *The Selberg Trace Formula and Related Topics* (edited by D. Hejhal, P. Sarnak and A. Terras), Contemporary Mathematics 53, Amer. Math. Soc., 1986.

[3] E. Hecke, *Mathematische Werke*, Vandenhoeck und Ruprecht, Göttingen 1983.

[4] D. Hejhal, *The Selberg Trace Formula for* PSL (2, *R*), Vol. II, Lecture Notes in Mathematics 1001, Springer-Verlag, New York 1983.

[5] H. Huber, *Über die Darstellungen der Automorphismengruppe einer Riemannschen fläche in den Eigenräumen des Laplace-operators*, Comment. Math. Helvetici 52 (1977), 177–184.

[6] S. Lang, *Elliptic Functions*, Springer-Verlag, New York.

[7] H. Saito, *On the representation of* SL_2 (F_q) *in the spaces of Hilbert modular forms*, J. Math. Kyoto Univ. 15 (1975), 101–128.

[8] P. Sarnak, *Class numbers of indefinite binary quadratic forms*, J. Number Theory 15 (1982), 229–247.

[9] J. Stopple, *A Functional Equation for some Selberg Zeta Functions*, Thesis, University of California at San Diego, 1986.

[10] — *Some Explicit Cases of the Selberg Trace Formula for Vector Valued Functions*, to appear in Trans. Amer. Math. Soc.

[11] S. Tanaka, *Construction and classification of irreducible representations of special linear group of the second order over a finite field*, Osaka J. Math. 4 (1967), 65–84.

MATHEMATICS DEPARTMENT
UNIVERSITY OF CALIFORNIA
Santa Barbara, CA 93 106
USA

Received on 5.11.1987
and in revised form on 30.5.1988 (1764)

ACTA ARITHMETICA
LIV (1989)

Galois groups of trinomials

by

STEPHEN D. COHEN (Glasgow)

1. Introduction. Let $f(X)$ denote a trinomial of the form

(1) $$f(X) = X^n + aX^r + b,$$

where a and b are rational integers. We always assume that f is irreducible over Q which implies that $G(f)(= G_Q(f))$, the Galois group of f over Q, is a transitive subgroup of the full symmetric group S_n acting on the zeros of f. Various authors, including Uchida [12], Yamamoto [13], Ohta [9] and Nart and Vila [8] have shown that, when $r = 1$, then, under certain specific simple conditions, $G(f) = S_n$ itself. (See also Yamamura [14].)

Recently, H. Osada [10], [10a], in extending these results, has shown that for arbitrary r, necessarily with n, r co-prime, i.e.

(2) $$(n, r) = 1,$$

a similar conclusion can be drawn under conditions which we summarise.

Let $d = (a, b)$ and put $a = da_0$, $b = db_0$. Assume that

(3) $$(a, n) = 1,$$

(4) $$d = c^n \quad \text{for some integer } c,$$

(5) $$d \text{ is a unitary divisor of } b, \text{ i.e. } (d, b_0) = 1,$$

(6) $$(r(n-r), b_0) = 1.$$

Then $G(f) = S_n$ in either of the following two situations.

I. $b_0 = b_1^r$ for some integer b_1 (e.g. $r = 1$) or $r = 2$.

II. For some prime p, $p \| b_0$ (i.e. $p | b_0$ but $p^2 \nmid b_0$) and the integer $|D_0(f)|$ is a non-square, where

$$D_0(f) = n^n b_0^{n-r} + (-1)^{n-1} r^r (n-r)^{n-r} a_0^n d^r$$

is related to the discriminant $D(f)$ of f by

$$D(f) = (-1)^{n(n-1)/2} b_0^{r-1} d^{n-1} D_0(f).$$

(The restriction of r to certain values in [10] was dispensed with in [10a].)