где \( \vartheta_f(t) \) — якобинная аппроксимация; \( \vartheta_{2k}(n) \) — сумма синусоидальных рядов Харди, отвечающего сумме 2к квадратов целых чисел; \( \vartheta_l^0 \) — постоянные, подобравшиеся надлежащим образом; \( l = \left\lceil \frac{2k-1}{8} \right\rceil \). Приравнивая коэффициенты при \( e^{int} \) в обоих частях этого тождества, получаем формулу для \( r_{2k}(n) \), выписанную выше.

Мы предполагаем, что функциональным эквивалентом формулы для арифметической функции \( r(n, F_4) \) будет тождество

\[
\vartheta(t, F_4) = E(t, F_4) + \sum_{i=1}^{l} \vartheta_i \vartheta(t, F_{k-2-2i}, \vartheta_{k+z_i-2i}),
\]

где \( l = \sum_{n=1}^{k} \left\lceil \frac{k}{6n} \right\rceil ; \vartheta_i^0 \) — постоянные, которые следует подбирать надлежащим образом. Это действительно так при \( 2 \leq k \leq 17 \), 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 \( r(n, F_4) \) следует из упомянутых тождеств приравниванием в их обеих частях коэффициентов при \( e^{it} \) Желательно доказать, что тождество (*) имеет место при всех \( k \geq 2 \) или опровергнуть это предположение.

**Литература**

1. V. Bougygine, 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. Дижон, Введение в теорию чисел. Обработанный перевод с английского А. З. Валлип, Тбилиси 1941.
4. Г. А. Ломазов, О решении чисел суммами квадратов, Тр. Тбилис. матем. ин-та им. А. М. Раззакова, 16 (1948), 231-275.
6. — О параллельных диагональных чисел и группах чисел, Тр. Тбилис. матем. ин-та им. А. М. Раззакова, 57 (1977), 63-81.
7. — О представлении чисел суммами квадратических форм \( x_1^2 + x_2^2 + x_3^2 + x_4^2 \), Тезисы докладов Всесоюзной конференции, "Теория чисел и ее приложения" (17-19 сентября 1983 г., Тбилис), с. 140.

Поступило 21.5.1987

(1725)
Let \( \psi \) be a virtual character of the group defined by
\[
\psi(g) = \text{trace}(\pi^+(g)) - \text{trace}(\pi^- (g)).
\]
From tables [11] we see that
\[
\psi(g) = \begin{cases} 
\sqrt{q} \left( \frac{x}{q} \right) & \text{if } g \in \text{SL}(2, F_q) \text{ is conjugate to a matrix } \pm \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}, \\
0 & \text{otherwise.}
\end{cases}
\]

2. The functional equation. The Selberg zeta function is defined by
\[
Z(s, \psi) = \prod_{P \in \pi} \prod_{k=0}^{\infty} \det(1 - \psi(P) N(P)^{-s-k}).
\]
Here \( \pi \) is any finite dimensional representation of \( \text{SL}(2, \mathbb{Z}) \), \( \pi \) is a primitive hyperbolic conjugacy class in \( \text{SL}(2, \mathbb{Z}) \), and \( N(P) \) is \( \psi \), where \( \psi \) is the larger eigenvalue of \( P \). The logarithmic derivative of \( Z(s, \psi) \) 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 \( \pi \) is a representation of \( \text{SL}(2, F_q) \), it is known (see [5], [10]) that the multiplicity of a zero \( s_0 \) of \( Z(s, \psi) \) is equal to the multiplicity of \( \phi \) for the action of \( \text{SL}(2, \mathbb{Z}) \) 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 \( \pi^+ \) and \( \pi^- \) by considering the quotient of Selberg zeta functions
\[
Z(s, \psi) = Z(s, \pi^+) / Z(s, \pi^-).
\]
From [10] we know that \( \pi^+ \) and \( \pi^- \) are both \((q+1)/2\) dimensional, and each gives a single continuous spectrum of representations of \( \text{SL}(2, \mathbb{Z}) \), i.e.,
\[
c_{\pi^+} = c_{\pi^-} = 1 \text{ in the notation of [10].}
\]
The corresponding scattering matrices are
\[
\Phi(s, \pi^+) = \left( \frac{\pi^+}{q} \right)^{2s-1} \Gamma(1-s) \begin{bmatrix} L(2-2s, \frac{\star}{q}) \\ L(2s, \frac{\star}{q}) \end{bmatrix},
\]
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 \( \text{trace}(\gamma) < 2 \Rightarrow \text{trace}(\gamma) \neq \pm 2(q) \) so \( \psi(\gamma) = 0 \) for \( \gamma \) elliptic in \( \text{SL}(2, \mathbb{Z}) \).

All that remains is the parabolic classes contribution to the discrete spectrum. Suppose \( \pi^+ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \) has eigenvalues \( \{\ldots, e^{2n\pi i}, \ldots\} \) and \( \pi^- \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \) has eigenvalues \( \{\ldots, e^{2(n+1)\pi i}, \ldots\} \). Then
\[
Z(1-s, \psi) = Z(s, \psi) \exp\{2(1-s) \sum_{\gamma \neq 0} \log|1-e^{2\pi i \gamma}| - \sum_{\gamma \neq 0} \log|1-e^{2\pi i \gamma}| \}.
\]
From [10] we know the eigenvalues of \( \pi^+ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \) are all nontrivial \( q \) roots of 1 corresponding to squares and nonsquares respectively in \( F_q^* \). Since \( 1-e^{-2\pi i \gamma} = 2\sin(\pi \gamma) \) we see that
\[
Z(1-s, \psi) = Z(s, \psi) \exp\{2(1-2s) \sum_{\gamma = 1}^{q-1} \frac{\gamma}{q} \log|1-e^{-2\pi i \gamma}| \}.
\]
By the Dirichlet class number formula,
\[
Z(1-s, \psi) = Z(s, \psi) e^{2\pi i (2s-1)}
\]
where \( k \) is the narrow class number, and \( \epsilon \) the fundamental positive norm unit in \( \mathcal{O}(\sqrt{q}) \).

3. The trace formula. We now consider the logarithmic derivative
\[
(3.1) \quad \frac{Z'(s, \psi)}{Z(s, \psi)} = \sum_{P \in \pi} \log NP \sum_{k=0}^{\infty} \frac{1}{N(P)^{s+k}}
\]
Define a map \( \varphi \) from matrices \( P \) to quadratic forms by
\[
\varphi \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & -c \\ b & -d \end{bmatrix},
\]
where \( v = \gcd(b, d-a, c) \). Conversely a form \( [a, b, c] \) with discriminant \( D = b^2 - 4ac \) is mapped to
\[
P = \begin{bmatrix} t + \varphi \beta \mu \\ w \end{bmatrix}
\]
where \( t^2 - u^2 \cdot D = 4 \) 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 \( \varphi \) is a 2-1 map (since \( \varphi(P) = \varphi(-P^-1) \)) and \( \varphi \) 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 \( \psi \) in Section 1 it is easy to see that

\[
\psi(P^k) = \begin{cases} 
\left( \frac{kuzz}{q} \right) \sqrt{-q} & \text{if } qD, \\
0 & \text{if } q \not| D.
\end{cases}
\]

Thus we have (3.1) reduces to

\[
2\sqrt{q} \sum_{d|D} \sum_{k=1}^{\infty} \sum_{[a, b, c] \text{ with } \text{disc}, b \not| D} \left( \frac{kuz}{q} \right) (NP \text{ terms}) \sum_{a, b, c} \left( \frac{a}{q} \right).
\]

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

\[ [\alpha, \beta, \gamma] \circ [\alpha', \beta', \gamma'] = [\alpha \alpha', \beta \beta', \gamma \gamma']. \]

If \( D = qd'^2 \) then we have \( qd'^2 \equiv \beta^2 \mod 4\alpha \) so \( \left( \frac{a}{q} \right) = \left( \frac{d'}{\alpha} \right) = 1 \) for all classes (recall \( q \equiv 1 \mod 4 \)). 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 \( \varepsilon_d = \left( \frac{t + u\sqrt{dd'}}{2} \right) \) be the unit \( Q(\sqrt{q}) \) corresponding to the Pell solution \( t^2 - u^2q^2d'^2 = 4 \), and let \( h(qd'^2) \) be the class number of forms. We now have (3.2) equals

\[
4\sqrt{q} \sum_{d=1}^{\infty} h(qd'^2) \log \varepsilon_d \sum_{k=1}^{\infty} \left( \frac{kuz}{q} \right) \varepsilon_d(q^{-1/2} \varepsilon_{d^{-1/2}}).
\]

From Lang [5] we know

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

and

\[
\log \varepsilon_d = \log \varepsilon \left( \frac{1}{2}, \frac{d}{p} \right),
\]

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

\[
Z'(s, \psi) = 4h \log \varepsilon \sqrt{q} \sum_{d=1}^{\infty} \prod_{p|d} \left( 1 - \left( \frac{p}{q} \right) \right) \sum_{k=1}^{\infty} \left( \frac{kuz}{q} \right) \varepsilon_d(q^{-1/2} \varepsilon_{d^{-1/2}}).
\]

We want to group all terms of the form \( \varepsilon_d = \varepsilon^n \) for \( n = 1, 2, \ldots \), so write

\[
\varepsilon^n = \frac{t(n) + f(n)\sqrt{q}}{2} \quad \varepsilon^n = \frac{t + u\sqrt{q}d^{-2}}{2} \quad \varepsilon = \frac{t + u\sqrt{q}d^{-2}}{2}
\]

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

\[
\sum_{k=1}^{\infty} \left[ \sum_{j=1 \text{ odd}}^{\infty} \left( \frac{k}{q} \right) \sqrt{j} \right] \sqrt{q} \sum_{k=1}^{\infty} \left( \frac{kuz}{q} \right) \varepsilon_d(q^{-1/2} \varepsilon_{d^{-1/2}}). \]

Since \( t_d \equiv \pm 2(q) \) equating (3.2) and (3.3) gives

\[
\left( \frac{kuz}{q} \right) = \left( \frac{f(n)/d}{q} \right).
\]

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

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

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

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

and we have proved the following

**THEOREM.** For \( \psi \) as in Section 1,

\[
Z(s, \psi) = \left( 1 - \varepsilon^{-1} \right) 2h.
\]

(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 \( s = 1/2 + k\pi i / \log \varepsilon \) for \( k \in \mathbb{Z} \) 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 \( \left( \frac{a}{q} \right) \), the Frobenius reciprocity theorem implies they transform under \( \Gamma_0(2) \) according to either \( \pi^+ \) or \( \pi^- \).

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 \( \left( \frac{a}{q} \right) \). 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


Galois groups of trinomials

by

STEPHEN D. COHEN (Glasgow)

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

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

where $a$ and $b$ are rational integers. We always assume that $f$ is irreducible over $\mathbb{Q}$ which implies that $G(f) = G_0(f)$, the Galois group of $f$ over $\mathbb{Q}$, 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. Osaka [10], [10a], in extending these results, has shown that for arbitrary $r$, necessarily with $n, r$ co-prime, i.e.

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

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

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

$$d = c^n$$

for some integer $c$.

$d$ is a unitary divisor of $b$, i.e. $(d, b_0) = 1$.

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

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

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

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

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

$$D(f) = (-1)^{n+1} b_0^{n-1} d_{n-1} D_0(f).$$

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