J. reine angew. Math. **544** (2002), 13—24

Journal für die reine und
angewandte Mathematik

Analytic ranks of elliptic curves over cyclotomic fields

By *Gautam Chinta* at Providence

---

1. Introduction

Let $L(s,E)$ be the L-function of an elliptic curve defined over $\mathbb{Q}$, and let $L(s,E,\chi)$ be the L-function twisted by a primitive Dirichlet character χ. It is of interest to know that many of the $L(s,E,\chi)$ are nonzero at the central point $s = 1/2$ for χ ranging over some set of primitive characters. In particular, letting K_q denote the cyclotomic extension of $\mathbb{Q}$ obtained by adjoining q^{th} roots of unity, the weak form of the conjecture of Birch and Swinnerton-Dyer equates the order of vanishing of

$$\prod_{\chi \bmod q} L(s,E,\chi) \tag{1}$$

at $s = 1/2$ with the rank of $E(K_q)$, the set of K_q-rational points of the elliptic curve. In (1) the product is taken over all Dirichlet characters $\bmod\, q$. We call

$$\operatorname*{ord}_{s=1/2}\left(\prod_{\chi \bmod q} L(s,E,\chi)\right)$$

the *analytic rank* of $E(K_q)$.

The fact that there are $\phi(q)$ terms in the above product together with the observation that $L(s,E,\chi)$ can vanish to order at most $O(\log q)$ at the central point gives us the trivial bound

$$\text{analytic rank of } E(K_q) \ll q\log q. \tag{2}$$

Assuming the generalized Riemann Hypothesis, R. Murty [1] gives the conditional bound

$$\text{analytic rank of } E(K_q) \leqq q/2 + o(1).$$

In subsequent work, T. Stefanicki [6] establishes the weaker, unconditional result that

$$\#\{\chi \bmod q\colon L(1/2,f,\chi) \neq 0\} \gg q/\log q.$$

However, this result is too weak to improve on the trivial bound (2) given above. (We note however that Stefanicki's method works also for Maass forms.)

Our first main result is

Theorem 1. *Let E be an elliptic curve defined over* $\mathbb{Q}$ *of conductor N. For any* $\varepsilon > 0$ *and q a sufficiently large prime* (*in terms of N and* ε),

$$\textit{analytic rank of } E(K_q) < q^{7/8+\varepsilon}.$$

Here K_q *is again the cyclotomic field obtained by adjoining the* q^{th} *roots of unity.*

The proof relies heavily on the arithmetic nature of the central values of the twisted L-functions. The main idea is that $L(1/2, E, \chi)$ is nonvanishing if and only if $L(1/2, E, \chi^\sigma)$ is nonvanishing for all Galois conjugates χ^σ of χ (see e.g. [4], [5]). This method was originally used by Rohrlich [3] to show that almost all $L(1/2, E, \chi)$ are nonzero for primitive χ unramified outside a given finite set of primes. Thus the Theorem 1 may be seen as an extension of Rohrlich's result to characters of prime modulus.

Rohrlich shows that a particular twisted L-function is nonzero by showing that the average

$$\sum_\sigma L(1/2, E, \chi^\sigma)$$

is nonzero. The method used in our proof of Theorem 1 is identical to Rohrlich's with one major difference: instead of the Galois average above, we look at a certain linear combination of the twisted L-functions

$$\sum_\sigma c_\sigma L(1/2, E, \chi^\sigma),$$

where the coefficient c_σ is chosen to be the "mollifying polynomial" of $L(s, E, \chi^\sigma)$ at $s = 1/2$. These mollified Galois averages turn out to be essential in the case of prime modulus because the character sums which arise do not afford as much cancellation as those considered by Rohrlich.

As an application of his result, Rohrlich proves that if E is an elliptic curve defined over $\mathbb{Q}$ with complex multiplication, then $E(K_\infty)$ is finitely generated, where K_∞ is the maximal abelian extension of $\mathbb{Q}$ unramified outside a finite set of primes P. Thus it becomes of interest to ask for bounds for the rank of $E(K_\infty)$. When P consists of a single prime p relatively prime to the conductor of E, denote by $\eta(p)$ the smallest $k \geqq 0$ such that $L(1/2, E, \chi) \neq 0$ for all primitive Dirichlet characters of conductor p^j with $j > k$. In [2], Rohrlich shows that

$$\eta(p) \ll p/\log p.$$

(Note: the implicit constant depends on E.) We use the methods developed in proving Theorem 1 above to prove

Theorem 2. *Let E be an elliptic curve defined over $\mathbb{Q}$. Then,*

$$\eta(p) \ll 1,$$

with the implicit constant depending on E.

Acknowledgments. The author is grateful to Prof. Dorian Goldfeld for his guidance and advice and to the referee for closely reading the paper and simplifying the proof of Proposition 1. I would also like to thank the Sloan Foundation for their support in the final year of my graduate studies.

2. Preliminaries

Let E be an elliptic curve defined over $\mathbb{Q}$. Due to the work initiated in Wiles and Taylor-Wiles ([8], [7]), we know that E is modular. Therefore, $L(s,E)$ coincides with the L-function of a holomorphic newform f of weight 2 for the group $\Gamma_0(N)$ with rational Fourier coefficients,

$$f(z) = \sum_{n \geqq 1} \lambda_n e^{2\pi i n z}.$$

The associated L-function is given by

$$\begin{aligned} L(s,f) &= \sum_{n \geqq 1} \lambda_n n^{-1/2} n^{-s} \\ &= \sum_{n \geqq 1} b_n n^{-s}, \end{aligned}$$

say.

Let q be an odd prime power, $(q,N) = 1$. For χ a Dirichlet character mod q we define the twisted L-functions

$$L(s,f,\chi) = \sum_{n \geqq 1} \chi(n) b_n n^{-s}.$$

These Dirichlet series are valid for $\mathrm{Re}(s) > 3/2$. The completed L-functions defined by

$$\Lambda(s,f,\chi) = \left(\frac{q\sqrt{N}}{2\pi}\right)^s \Gamma(s+1/2) L(s,f,\chi)$$

have analytic continuations to the plane, are bounded in vertical strips and satisfy the functional equation

$$\Lambda(s,f,\chi) = w_\chi \Lambda(1-s,f,\bar{\chi}), \quad |w_\chi| = 1.$$

The "root number" w_χ has a simple expression in terms of Gauss sums which we will recall at the appropriate time. Finally, we have the Euler product

$$L(s,f,\chi) = \prod_p \left(1 - \alpha_p \chi(p) p^{-s}\right)^{-1} \left(1 - \beta_p \chi(p) p^{-s}\right)^{-1},$$

where $|\alpha_p| = |\beta_p| = 1$ for $p \nmid N$ and $|\alpha_p| \leqq 1$, $\beta_p = 0$ for $p | N$.

We will average the twisted L-functions over the Galois conjugates of χ. More precisely, let D_q be the group of Dirichlet characters $\bmod q$. This is a cyclic group of order $\phi(q)$, where ϕ is the Euler-ϕ function. Suppose $\chi \in D_q$ has order $\phi(q)/d, d \mid \phi(q)$. Let $\mathbb{Q}[\chi]$ be the extension of $\mathbb{Q}$ generated by the image of χ, with Galois group $G = \mathrm{Gal}(\mathbb{Q}[\chi]/\mathbb{Q})$. Thus

$$\mathbb{Q}[\chi] = \mathbb{Q}[\zeta],$$

where ζ is a primitive $\phi(q)/d^{\text{th}}$ root of unity, and the Galois group G has order $\phi\big(\phi(q)/d\big)$. Indeed, any $\sigma \in G$ is completely determined by what it does to ζ, and moreover, if σ generates G, the image of ζ under σ may be any one of the $\phi\big(\phi(q)/d\big)$ primitive $\phi(q)/d^{\text{th}}$ roots of unity.

We define

$$\chi_{\text{av}}(n) = \frac{1}{|G|} \sum_{\sigma \in G} \chi^{\sigma}(n)$$

and

$$\tilde{\chi}_{\text{av}}(n) = \frac{1}{|G|} \sum_{\sigma \in G} w_{\chi^{\sigma}} \overline{\chi^{\sigma}}(n).$$

Note that for a generator g of $(\mathbb{Z}/q\mathbb{Z})^*$, $\chi^{\sigma}(g)$ ranges over the primitive $\phi(q)/d^{\text{th}}$ roots of unity as σ ranges over elements of G.

Rohrlich's idea was to consider

$$\begin{aligned} L(s, f, \chi_{\text{av}}) &= \frac{1}{|G|} \sum_{\sigma \in G} L(s, f, \chi^{\sigma}) \\ &= \sum_{n \geqq 1} \chi_{\text{av}}(n) b_n n^{-s}. \end{aligned}$$

Exploiting the cancellations in the averaged characters, he was able to show that the Galois average of the central values is nonzero:

$$L(1/2, f, \chi_{\text{av}}) \neq 0.$$

Then by the theorem of Shimura (see [4], [5]), it follows that each individual central value must be nonzero.

The idea of our arguments is very similar. The only difference is that we wish to average over smaller Galois orbits. Therefore there is now less cancellation among the averaged characters. We compensate for this with an additional analytic tool—the mollifier, to be introduced in Section 3.

We conclude this section with some crude bounds for the averaged Galois characters.

Proposition 1. *Let q be an odd prime power and let $d \mid \phi(q)$. Let χ be a Dirichlet character* mod *q of order $\phi(q)/d$. Then*

(i) $\chi_{\text{av}}(n) = \mu\big(\mathrm{ord}(n^d)\big)/\phi\big(\mathrm{ord}(n^d)\big)$,

(ii) $\sum_{n \bmod q} |\chi_{\mathrm{av}}(n)| \leqq \sigma_1(d)2^{\nu(\phi(q))}$,

(iii) $\tilde{\chi}_{\mathrm{av}}(n) \leqq 2^{\nu(\phi(q))+1}\sigma_1(d)/\sqrt{q}$.

Here $\nu(n)$ *is the number of distinct prime divisors of* n, $\mathrm{ord}(n)$ *denotes the order of* n *in* $(\mathbb{Z}/q\mathbb{Z})^*$, *and* $\sigma_1(d) = \sum_{a|d} a$ *is the divisor sum function.*

Proof. We begin by establishing the following character sum:

$$\sum_{a\in(\mathbb{Z}/c\mathbb{Z})^\times} e(ka/c) = \frac{\mu(c/k)\phi(c)}{\phi(c/k)}, \quad \text{for } k|c. \tag{3}$$

Noting that the value of the summand in equation (3) depends only on the value of a modulo c/k,

$$\sum_{a\in(\mathbb{Z}/c\mathbb{Z})^\times} e(ka/c) = \frac{\phi(c)}{\phi(c/k)} \sum_{a\in(\mathbb{Z}/(c/k)\mathbb{Z})^\times} e\left(\frac{a}{c/k}\right). \tag{4}$$

Then the proof of equation (3) is completed by taking $c' = c/k$ in the formula for the classical Ramanujan sum:

$$\sum_{a\in(\mathbb{Z}/c'\mathbb{Z})^\times} e(a/c') = \mu(c').$$

Let χ be a Dirichlet character mod q of order $\phi(q)/d$. We compute

$$\chi_{\mathrm{av}}(n) = \frac{1}{\phi\left(\frac{\phi(q)}{d}\right)} \sum_{\sigma\in G} \chi^\sigma(n) = \frac{1}{\phi\left(\frac{\phi(q)}{d}\right)} \sum_{(a,\phi(q)/d)=1} e\big(a/\mathrm{ord}(n^d)\big).$$

(As before, σ ranges over $G = \mathrm{Gal}(\mathbb{Q}[\chi]/\mathbb{Q})$, and $\mathrm{ord}(n)$ denotes the order of n in the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$.) Hence, by equation (3),

$$\chi_{\mathrm{av}}(n) = \frac{\mu\big(\mathrm{ord}(n^d)\big)}{\phi\big(\mathrm{ord}(n^d)\big)}.$$

Taking absolute values and summing over n mod q, this becomes

$$\begin{aligned}
\sum_{1\leqq n<q} |\chi_{\mathrm{av}}(n)| &= \sum_{\substack{k|\phi(q)\\ k \text{ squarefree}}} \#\{n\colon n^d \text{ has order } k\}/\phi(k) \\
&= \sum_{\substack{k|\phi(q)\\ k \text{ squarefree}}} \#\left\{n\colon \frac{\mathrm{ord}(n)}{(d,\mathrm{ord}(n))} = k\right\}\Big/\phi(k) \\
&\leqq \sum_{\substack{k|\phi(q)\\ k \text{ squarefree}}} \frac{1}{\phi(k)}\left[\sum_{\lambda|d} \phi(k\lambda)\right] \qquad (5)
\end{aligned}$$

$$\leqq \sum_{\substack{k \mid \phi(q) \\ k \text{ squarefree}}} \frac{\phi(k)}{\phi(k)} \left[\sum_{\lambda \mid d} \lambda\right]$$

$$\leqq \sigma_1(d) 2^{\nu(\phi(q))}.$$

The inequality in (5) deserves further comment. The set

$$\{n\colon \operatorname{ord}(n) = k(d, \operatorname{ord}(n))\}$$

is contained in the set

$$\bigcup_{\lambda \mid d} \{n\colon \operatorname{ord}(n) = k\lambda\}. \tag{6}$$

The number of elements in the cyclic group $(\mathbb{Z}/q\mathbb{Z})^\times$ of exact order m is $\phi(m)$, if $m \mid \phi(q)$, and 0 otherwise. Hence a bound for the cardinality of the set in (6) is

$$\sum_{\lambda \mid d} \phi(k\lambda).$$

This establishes the inequality (5).

We have proven the first two parts of the proposition. To prove part (iii), we first recall the definition of the root number:

$$w_\chi = \frac{\varepsilon_f \chi(N)}{q} \left[\sum\nolimits^* \chi(j) e(j/q)\right]^2,$$

where the sum is over $j \bmod q$, $(j, q) = 1$. Therefore, assuming $(n, q) = 1$ and $n\bar{n} \equiv 1$,

$$\begin{aligned}
\tilde{\chi}_{\mathrm{av}}(n) &= \frac{1}{\phi\left(\frac{\phi(q)}{d}\right)} \sum_\sigma w_\chi \overline{\chi^\sigma}(n) \\
&= \frac{\varepsilon_f}{q} \sum_{j,k}\nolimits^* e\left(\frac{j+k}{q}\right) \frac{1}{\phi\left(\frac{\phi(q)}{d}\right)} \sum_\sigma \chi^\sigma(\bar{n}) \chi^\sigma(N) \chi^\sigma(jk) \\
&= \frac{\varepsilon_f}{q} \sum_{j,k}\nolimits^* \chi_{\mathrm{av}}(\bar{n}Njk) e\left(\frac{j+k}{q}\right) \\
&= \frac{\varepsilon_f}{q} \sum_{r \bmod q} \chi_{\mathrm{av}}(\bar{n}Nr) \sum_{jk \equiv r \pmod q} e\left(\frac{j+k}{q}\right).
\end{aligned}$$

Taking absolute values and using the Weil bound on the Kloosterman sum, we get after a change of variable,

$$|\tilde{\chi}_{\mathrm{av}}(n)| \ll q^{-1/2} \sum_{r \bmod q} |\chi_{\mathrm{av}}(r)|.$$

Now (iii) follows from (ii), and the proof of the proposition is complete. □

3. The mollifier

The mollifier is a tool for controlling the variations in size of the absolute value of the central values $L(1/2, f, \chi)$ as χ runs over the set of primitive characters of some fixed modulus.

First note that the Euler product

$$L(s, f, \chi) = \prod_p \bigl(1 - \alpha_p \chi(p) p^{-s}\bigr)^{-1} \bigl(1 - \beta_p \chi(p) p^{-s}\bigr)^{-1},$$

where $|\alpha_p| = |\beta_p| = 1$ for $p \nmid N$ and $|\alpha_p| \leqq 1$, $\beta_p = 0$ for $p | N$, immediately gives us a Dirichlet series representation for the inverted L-series:

$$L(s, f, \chi)^{-1} = \sum_{n=1}^{\infty} c_n \chi(n) n^{-s},$$

where (letting $n = kl^2m$, $(k, l) = (l, m) = (k, m) = 1$, with k squarefree, m cubefull)

$$c_n \chi(n) = \mu(k) \mu(m) \chi(n) \varepsilon_N(l) b_k.$$

Here, ε_N is the trivial Dirichlet character mod N.

We now define the *mollifier polynomial of length X* to be

$$M_X(s, \chi) = \sum_{n \leqq X} c_n \chi(n) n^{-s}.$$

Whereas the Dirichlet series for the inverted L-series converges absolutely only for $\mathrm{Re}(s) > 1$, the mollifying polynomial is an entire function which we hope in some sense approximates $L(s, f, \chi)^{-1}$ at the central point $s = 1/2$.

For $\mathrm{Re}(s) > 1$,

$$L(s, f, \chi) M_X(s, \chi) = \sum_{n=1}^{\infty} a_n \chi(n) n^{-s},$$

where

$$a_n = a_n(X) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } 1 < n \leqq X, \\ O\bigl(\sigma_0(n)^3\bigr) & \text{if } n \geqq X, \end{cases}$$

where $\sigma_0(n)$ is the number of divisors of n. (This final estimation uses the Ramanujan bound $b_n \ll \sigma_0(n)$.)

4. The approximate functional equation

The central point of the Dirichlet series $L(s, f, \chi)$ is outside the region of absolute convergence. There is a general method for expressing an L-function as a rapidly convergent series at the central point. This method is known as the method of the approximate functional equation. We apply it to derive an expression for the product $L(s,f,\chi)M_X(s,\chi)$ at $s = 1/2$.

Consider the integral

$$\frac{1}{2\pi i}\int\limits_{(\frac{1}{2}+\varepsilon)} \Lambda\left(\frac{1}{2}+s,f,\chi\right)M_X\left(\frac{1}{2}+s,\chi\right)Y^s\frac{ds}{s}.$$

(The positive parameters X and Y will be chosen later.) Moving the contour of integration over to $\left(-\frac{1}{2}-\varepsilon\right)$ to pick up the pole at $s = 0$, using the functional equation, and then replacing the L-function by its defining series in the region of absolute convergence, we get

$$(7)\quad L\left(\frac{1}{2},f,\chi\right)M_X\left(\frac{1}{2},\chi\right) = e^{-2\pi/qY\sqrt{N}} + \sum_{n>X}\frac{a_n\chi(n)}{\sqrt{n}}\exp\left(\frac{-2\pi n}{qY\sqrt{N}}\right)$$
$$+\sum_{n\geqq 1}\sum_{1\leqq m\leqq X}\frac{b_nc_m}{\sqrt{nm}}\bar{\chi}(n)\chi(m)w_\chi\exp\left(\frac{-2\pi nY}{mq\sqrt{N}}\right),$$

where we have used the Mellin transform

$$e^{-t} = \frac{1}{2\pi i}\int\limits_{(\frac{1}{2}+\varepsilon)} t^{-s}\Gamma(s)\,ds.$$

As in Section 2, let $\mathbb{Q}[\chi]$ be the extension of $\mathbb{Q}$ generated by the image of χ, with Galois group $G = \mathrm{Gal}(\mathbb{Q}[\chi]/\mathbb{Q})$. Averaging (7) over G we obtain

$$(8)\qquad \frac{1}{|G|}\sum_{\sigma\in G}L\left(\frac{1}{2},f,\chi^\sigma\right)M_X\left(\frac{1}{2},f,\chi^\sigma\right) = \exp\left(\frac{-2\pi}{qY\sqrt{N}}\right)+S_1+S_2,$$

where

$$S_1 = \sum_{n>X}\frac{a_n\chi_{\mathrm{av}}(n)}{\sqrt{n}}\exp\left(-\frac{2\pi n}{qY\sqrt{N}}\right)$$

and

$$S_2 = \sum_{n\geqq 1}\sum_{1\leqq m\leqq X}\frac{b_nc_m}{\sqrt{nm}}\tilde{\chi}_{\mathrm{av}}(n\bar{m})\exp\left(\frac{-2\pi nY}{mq\sqrt{N}}\right).$$

(Here, $\bar{m}$ is defined by $m\bar{m}\equiv 1 \pmod{q}$ if $(m,q) = 1$ and is zero otherwise.) We choose the parameters X and Y to be

$$X = q^b,\quad Y = q^a$$

with a, b positive constants $b < a$ to be specified later.

5. Proof of Theorem 1

It remains to show that S_1 and S_2 are small when the parameters X and Y are appropriately chosen. We begin with S_2:

$$\begin{aligned}|S_2| &= \left|\sum_{n\geqq 1}\sum_{1\leqq m\leqq X}\frac{b_nc_m}{\sqrt{nm}}\tilde{\chi}_{\mathrm{av}}(n\bar{m})\exp\left(\frac{-2\pi nY}{mq\sqrt{N}}\right)\right| \\ &\ll \sum_{n\geqq 1}\sum_{1\leqq m\leqq X}\left|\frac{b_nc_m}{\sqrt{nm}}\tilde{\chi}_{\mathrm{av}}(n\bar{m})\exp\left(\frac{-2\pi nY}{qX\sqrt{N}}\right)\right| \\ &\ll \frac{2^{v(\phi(q))}\sigma_1(d)}{\sqrt{q}}X^{1/2+\varepsilon}\sum_{n=1}^{\infty}\frac{1}{n^{1/2-\varepsilon}}\exp\left(\frac{-2\pi nY}{qX\sqrt{N}}\right) \\ &\ll \frac{2^{v(\phi(q))}\sigma_1(d)}{\sqrt{q}}X^{1+2\varepsilon}\left(\frac{q\sqrt{N}}{Y}\right)^{1/2+\varepsilon}.\end{aligned}$$

We have used the Ramanujan bounds $b_n, c_n \ll_\varepsilon n^\varepsilon$, and part (iii) of Proposition 2. Or, since $X = q^b$ and $Y = q^a$,

$$|S_2| \ll \frac{N^{1/4+\varepsilon/2}}{q^{a/2-b+\varepsilon(a-2b-1)}}2^{v(\phi(q))}\sigma_1(d). \tag{9}$$

We now turn to the sum S_1

$$\begin{aligned}|S_1| &= \left|\sum_{n>X}\frac{a_n\chi_{\mathrm{av}}(n)}{\sqrt{n}}\exp\left(-\frac{2\pi n}{qY\sqrt{N}}\right)\right| \\ &\leqq \sum_{X<n\leqq q}\Big|\quad\Big| + \sum_{q\leqq n\leqq q^c}\Big|\quad\Big| + \sum_{q^c\leqq n}\Big|\quad\Big| \\ &= \sum_{\mathrm{I}} + \sum_{\mathrm{II}} + \sum_{\mathrm{III}},\end{aligned}$$

say.

In the first sum, we use the Ramanujan bound on the coefficients:

$$\sum_{\mathrm{I}} \ll X^{\varepsilon-1/2}\sum_{n\leqq q}|\chi_{\mathrm{av}}(n)|,$$

and then appeal to part (ii) of Proposition 2 to conclude

$$\sum_{\mathrm{I}} \ll \frac{2^{v(\phi(q))}\sigma_1(d)}{q^{b/2-\varepsilon b}}. \tag{10}$$

Similarly, the Ramanujan bound and repeated applications of part (ii) of the proposition yield

$$\begin{aligned}\sum_{\mathrm{II}} &\leqq \sum_{k=1}^{\lfloor q^{c-1}\rfloor}\sum_{n=kq+1}^{(k+1)q}\left|\frac{a_n\chi_{\mathrm{av}}(n)}{\sqrt{n}}\right| \\ &\ll \sum_{k=1}^{\lfloor q^{c-1}\rfloor}(kq)^{\varepsilon-\frac{1}{2}}\sum_{n=kq+1}^{(k+1)q}|\chi_{\mathrm{av}}(n)| \\ &\ll 2^{v(\phi(q))}\sigma_1(d)q^{\varepsilon-1/2}\sum_{k=1}^{\lfloor q^{c-1}\rfloor}k^{\varepsilon-1/2}.\end{aligned}$$

Assuming that the constant c satisfies $1 < c < 2$, we get

$$\sum_{\mathrm{II}} \ll \frac{2^{\nu(\phi(q))}\sigma_1(d)}{q^{1-c/2-2\varepsilon}}. \tag{11}$$

Finally,

$$\begin{aligned}\sum_{\mathrm{III}} &\ll \sum_{n>q^c} n^{\varepsilon-1/2} e^{-2\pi n/(qY\sqrt{N})}\\ &\ll \frac{1}{q^{c/2-c\varepsilon}} \int_{q^c}^{\infty} e^{-2\pi t/(qY\sqrt{N})}\,dt\\ &\ll Yq^{1-c/2+c\varepsilon}\sqrt{N}\exp\left(-\frac{q^{c-1}}{Y\sqrt{N}}\right).\end{aligned}$$

Hence

$$\sum_{\mathrm{III}} \ll \exp\left(-\frac{q^{c-1-a-\varepsilon}}{\sqrt{N}}\right), \tag{12}$$

provided $a+1 < c < 2$. Further require that $0 < b < a/2$. Collecting the bounds from equations (9), (10), (11), and (12), we get

$$S_2 \ll \frac{N^{1/4+\varepsilon/2}}{q^{a/2-b-\varepsilon}} 2^{\nu(\phi(q))}\sigma_1(d)$$

and

$$S_1 \ll 2^{\nu(\phi(q))}\sigma_1(d)q^{\varepsilon}\cdot\max(q^{-b/2}, q^{c/2-1}) + \exp\left(-\frac{q^{c-1-a-\varepsilon}}{\sqrt{N}}\right).$$

Suppose that $\sigma_1(d) \leqq q^{\gamma}$, $\gamma < 1/8$. Then S_1 and S_2 go to zero as $q \to \infty$ under the following choice of a, b, and c:

$$a = 1/2 + b, \quad b = 2\gamma + 3\varepsilon, \quad c = 2 - 2\gamma - 3\varepsilon.$$

Moreover, with this choice of a, b, and c, we see that S_1 and S_2 are $o(1)$ provided

$$N \ll q^{1-8\gamma-6\varepsilon}.$$

We have proven

Theorem 3. *Let f be a newform of weight 2 for $\Gamma_0(N)$ with rational Fourier coefficients and associated L-function $L(s, f)$. Let q be an odd prime power prime, $(q, N) = 1$, and χ a Dirichlet character* mod q. *Then*

$$L(1/2, f, \chi) \neq 0,$$

provided

$$\sigma_1\left(\frac{\phi(q)}{\operatorname{ord}\chi}\right) \leqq q^{\gamma}, \quad \gamma < 1/8$$

and

$$q \gg_\varepsilon N^{1/(1-8\gamma-\varepsilon)}.$$

The implied constant depends only on ε *and* γ, *and* $\sigma_1(d)$ *is the divisor sum function*

$$\sum_{a|d} a = \sigma_1(d).$$

Now let d be a divisor of $\phi(q)$. There are $\phi(\phi(q)/d)$ Dirichlet characters $\bmod\, q$ of order $\phi(q)/d$. Hence the number of such characters is less than q/d. Since $\sigma_1(d) \ll_\varepsilon d^{1+\varepsilon}$, there exists a constant C_ε such that the condition

$$\sigma_1(d) \geqq q^\gamma$$

implies

$$d > C_\varepsilon q^{\gamma-\varepsilon}.$$

Therefore, for q a sufficiently large prime

$$\begin{aligned} \#\{\chi \bmod q\colon L(1/2, E, \chi) = 0\} &\leqq \sum_{\substack{d|\phi(q) \\ \sigma_1(d) \geqq q^\gamma}} \phi\left(\frac{\phi(q)}{d}\right) \\ &\leqq \sum_{\substack{d|\phi(q) \\ d > C_\varepsilon q^{\gamma-\varepsilon}}} q/d \\ &\ll q^{1-\gamma+\varepsilon}. \end{aligned}$$

Choosing γ sufficiently close to 1/8 concludes the proof of Theorem 1.

6. Proof of Theorem 2

Theorem 2 also follows quickly from Theorem 3. We first need

Lemma 1. *Let* χ *be a primitive Dirichlet character* mod p^n, *p an odd prime. Then,*

$$\operatorname{ord}(\chi) \geqq p^{n-1}.$$

Proof. First note that $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is a cyclic group of order $\phi(p^n) = p^n - p^{n-1}$ and

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}.$$

Since a finite group is (abstractly) isomorphic to its dual,

$$D_{p^n} \cong (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}, \tag{13}$$

where D_{p^n} is the dual to $(\mathbb{Z}/p^n\mathbb{Z})^\times$. (In other words, D_{p^n} is just the group of Dirichlet characters mod p^n defined above.)

The imprimitive characters in D_{p^n} are those induced from characters on $(\mathbb{Z}/p^{n-1}\mathbb{Z})^{\times}$. Hence there are

$$\phi(p^{n-1}) = p^{n-2}(p-1) \tag{14}$$

imprimitive characters in D_{p^n} and

$$\phi(p^n) - \phi(p^{n-1}) = p^{n-2}(p-1)^2 \tag{15}$$

primitive characters.

By virtue of the isomorphism 13, we may identify Dirichlet characters in D_{p^n} with pairs (χ_1, χ_2), where χ_1 is an additive character of $\mathbb{Z}/(p-1)\mathbb{Z}$ and χ_2 is an additive character of $\mathbb{Z}/p^{n-1}\mathbb{Z}$. There are $\phi(p^{n-1}) = (p-1)p^{n-2}$ additive characters on $\mathbb{Z}/p^{n-1}\mathbb{Z}$ of order p^{n-1}. Therefore there are $(p-1)^2 p^{n-2}$ pairs (χ_1, χ_2) as above of order *at least* p^{n-1}. By equation (14) an imprimitive character in D_{p^n} can have order *at most* $p^{n-2}(p-1)$. It follows that the $(p-1)^2 p^{n-2}$ Dirichlet characters of order at least p^{n-1} must all be primitive, and by equation (15) these must account for all the primitive characters in D_{p^n}. □

But Theorem 3 ensures that $L(1/2, f, \chi)$ is non-zero provided

$$\operatorname{ord}(\chi) \gg (p^n)^{7/8+\varepsilon}.$$

Equivalently, we need

$$p^{n-8-8n\varepsilon} \gg 1. \tag{16}$$

(The implicit constant depends on ε and N.) Following the notation of Theorem 2, denote by $\eta(p) = \eta_f(p)$ the smallest $k \geqq 0$ such that $L(1/2, f, \chi) \neq 0$ for all primitive Dirichlet characters of conductor p^j with $j > k$. From (16) we see that $\eta_p \ll 1$.

References

[1] *M. Ram Murty*, On simple zeros of certain L-series, in: Number theory, de Gruyter, Berlin (1990), 427–439.

[2] *David E. Rohrlich*, Courbes elliptiques, fonctions L, et tours cyclotomiques, in: Seminar on number theory, Talence 1983/1984, Exp. No. 14, 10. Univ. Bordeaux I, Talence 1984.

[3] *David E. Rohrlich*, On L-functions of elliptic curves and cyclotomic towers, Invent. Math. **75** (3) (1984), 409–423.

[4] *Goro Shimura*, The special values of the zeta functions associated with cusp forms, Comm. Pure Appl. Math. **29** (6) (1976), 783–804.

[5] *Goro Shimura*, On the periods of modular forms, Math. Ann. **229** (3) (1977), 211–221.

[6] *Tomasz Stefanicki*, Non-vanishing of L-functions attached to automorphic representations of GL(2) over Q, J. reine angew. Math. **474** (1996), 1–24.

[7] *Richard Taylor* and *Andrew Wiles*, Ring-theoretic properties of certain Hecke algebras, Ann. Math. (2) **141** (3) (1995), 553–572.

[8] *Andrew Wiles*, Modular elliptic curves and Fermat's last theorem, Ann. Math. (2) **141** (3) (1995), 443–551.

Department of Mathematics, Box 1917, Brown University, Providence, RI 02912
e-mail: chinta@math.brown.edu

Eingegangen 5. Februar 2001