

ON LANDAU-SIEGEL ZEROS

BEN GREEN

1. INTRODUCTION

In this note we give a variant of the OpenAI proof [3] of no Landau-Siegel zeros. The proof was obtained by a ‘vibemathing’ session with ChatGPT 6 Astra followed by rewriting the argument myself. No human originality is claimed. The approach here has, arguably, two advantages over the OpenAI one. First, it avoids the rather unnatural passage to a biquadratic field $\mathbf{Q}(\sqrt{d}, \sqrt{2})$, and instead works entirely in $\mathbf{Q}(\sqrt{d})$. Second, it replaces the linear-algebraic interpolation argument of that paper with a proof that some readers may find more natural and straightforward. While both arguments compare archimedean and p -adic sizes of a certain determinant, the one in [3] is specified by an algorithm, whereas the one considered here is explicit. We note that expositions of the original OpenAI proof have already been given by Banks [1] and Kerr [2]. Both have their advantages; Banks gives explicit constants, while Kerr’s argument is only 6 pages modulo a result of Masser.

Let χ be a primitive, nonprincipal real Dirichlet character of sufficiently large conductor q , given by $\chi(p) = (d | p)$ for some d , for all $p \nmid q$. Let C be a sufficiently large even integer.

Theorem 1.1. *Set $X := q^C$. Then we have*

$$\sum_{\substack{p \leq X \\ \chi(p) = -1}} \frac{\log p}{p} \leq \left(\frac{1}{2} + O\left(\frac{1}{C}\right)\right) \log X + O_C(1).$$

Note that the trivial bound for the LHS is essentially $\log X$. That Theorem 1.1 implies that no Landau-Siegel zero can exist is a standard piece of analytic number theory, described perfectly well in [3].

2. SKETCH OF THE PROOF

Set $K = \mathbf{Q}(\sqrt{d})$ and $X = q^C$. We will also require integer parameters R, S, N, J which, with hindsight, we take to have values

$$R = X, \quad S = J = \lfloor X/C \rfloor, \quad \text{and} \quad N = 2X^{1/2}. \quad (2.1)$$

We first describe some row vectors $v_{r,s} \in K^{N^2 J}$. These will be given by

$$v_{r,s} := \left(\partial_z^j (z^r (z')^s) \Big|_{(z,z')=P_i} \right)_{1 \leq i \leq N^2, 0 \leq j < J},$$

where the $P_i \in \mathbf{C}^2$ are the points $(x + y\sqrt{d}, x - y\sqrt{d})$, with $x, y \in \mathbf{Z}$ and $0 \leq x, y < N$ (listed in some arbitrary order).

We will consider these $v_{r,s}$ for pairs (r, s) with $0 \leq r < R$ and $0 \leq s < S$. Finally, consider the Gram matrix G , which is an $(RS) \times (RS)$ matrix with entries $\langle v_{r,s}, v_{r',s'} \rangle$, all of which are (rational) integers. Here, the inner product on $K^{N^2 J}$ is extended coordinatewise from the pairing on K given by $\langle \alpha, \beta \rangle = \text{tr}_{K/\mathbf{Q}}(\alpha \bar{\beta})$, where the bar is complex conjugation.

We will prove the following three things about $\det G$:

- (1) $\det G \in \mathbf{Z}_{>0}$;

(2) An (archimedean) upper bound for $\det G$;

(3) A lower bound for the p -adic valuation e_p of $\det G$, for primes p with $p \leq X$ with $\chi(p) = -1$.

Since $\det G \neq 0$, we have $\prod_p p^{e_p} \leq \det G$ and this (followed by a short calculation) will lead to our theorem.

Remark. Instead of considering the Gram matrix G , one could run a very similar argument using a non-singular $(RS) \times (RS)$ submatrix of the matrix formed by the $v_{r,s}$. The existence of such a matrix follows from Lemma 3.1 below.

3. THE GRAM MATRIX IS NONSINGULAR

Any Gram matrix is positive semi-definite, so the key part of (1) is to show that G is non-singular. By standard linear algebra, this is equivalent to the rows $v_{r,s}$ being linearly independent. For this, almost nothing specific is used about the points P_i as defined above, and indeed we will prove the following general statement.

Lemma 3.1. *Let R, S, J, n be any positive integers. Suppose we have points $P_i := (z_i, z'_i)$, $i = 1, \dots, n$, in $\mathbf{C}^2$. Suppose that:*

- (1) *the z'_i are pairwise distinct, and*
- (2) *for every non-zero polynomial $F \in \mathbf{C}[z, z']$,*

$$\#\{i : F(P_i) = 0\} \leq J \deg F, \quad (3.1)$$

where $\deg F$ is the total degree of F .

Consider, for any $r, s \in \mathbf{Z}_{\geq 0}$, the vectors

$$v_{r,s} := (\partial_z^j (z^r (z')^s)|_{(z,z')=P_i})_{1 \leq i \leq n, 0 \leq j < J} \in \mathbf{C}^{nJ}.$$

Suppose that

$$nJ > 2RS + J(R + S). \quad (3.2)$$

Then the RS vectors $v_{r,s}$, $0 \leq r < R, 0 \leq s < S$, are linearly independent in $\mathbf{C}^{nJ}$.

Before turning to the proof, we remark on how this applies to our particular set of points P_i , namely the $(x + y\sqrt{d}, x - y\sqrt{d})$ with $0 \leq x, y < N$ (in some order), with the parameter choice in (2.1). In this setting, item (1) is obvious, while (2) is an immediate consequence of the Schwarz-Zippel lemma provided that $J \geq N$, which is the case for the choice of parameters (2.1). Finally, the condition (3.2) is satisfied with $n = N^2$ by the choice of parameters (2.1).

Proof of Lemma 3.1. Suppose not. Then there is a polynomial $F \in \mathbf{C}[z, z']$ of degree $\leq (R, S)$ in the variables z, z' such that

$$(\partial_z^j F)(P_i) = 0 \quad \text{for all } i = 1, \dots, n \text{ and } 0 \leq j < J. \quad (3.3)$$

Factor

$$F(z, z') = F_0(z') \prod_{\ell=1}^k F_\ell(z, z')$$

where the F_ℓ are irreducibles (not necessarily distinct) with $d_\ell := \deg_z F_\ell > 0$ for $\ell = 1, \dots, k$. In particular, each specialisation $F_\ell(z, z'_i)$ is not identically zero.

Let d'_ℓ be the z' -degree of F_ℓ for $0 \leq \ell \leq k$. Clearly

$$\sum_{\ell=1}^k d_\ell \leq R, \quad \sum_{\ell=0}^k d'_\ell \leq S. \quad (3.4)$$

We use some basic facts about resultants, for details of which the reader may consult Appendix A. In particular by Lemma A.1 we have

$$\text{ord}_{z=z_i} F_\ell(z, z'_i) \leq 1 + \text{ord}_{z'=z'_i} \text{Res}_z(F_\ell, \partial_z F_\ell). \quad (3.5)$$

Summing over i gives

$$\sum_{i=1}^n \text{ord}_{z=z_i} F_\ell(z, z'_i) \leq J(d_\ell + d'_\ell) + 2d_\ell d'_\ell \quad (3.6)$$

for each ℓ ; here we used that the number of i for which $F_\ell(z_i, z'_i) = 0$ is bounded above by $J(d_\ell + d'_\ell)$ (which is assumption (2)) together with the fact that the degree of the resultant is $\leq 2d_\ell d'_\ell$, which is (A.1).

Remove from $\{1, \dots, n\}$ the indices for which $F_0(z'_i) = 0$; there are at most d'_0 of these. For the remaining indices i , $F(z, z'_i)$ is not identically zero and so by (3.3) it has a zero of multiplicity at least J at $z = z_i$. We thus have

$$J(n - d'_0) \leq \sum_{\ell=1}^k \sum_{i=1}^n \text{ord}_{z=z_i} F_\ell(z, z'_i) \leq \sum_{\ell=1}^k (J(d_\ell + d'_\ell) + 2d_\ell d'_\ell) \leq J(R + S - d'_0) + 2RS,$$

where the final step follows using (3.4) and the crude bound $\sum_{\ell=1}^k d_\ell d'_\ell \leq (\sum_{\ell=1}^k d_\ell)(\sum_{\ell=1}^k d'_\ell)$. This gives $n \leq \frac{2RS}{J} + R + S$, which is contrary to the assumption (3.2). The result is proved. $\square$

4. ARCHIMEDEAN BOUND

In this section we give an upper bound on $\det G$. For this we use the Hadamard bound

$$\det G \leq \prod_{r,s} \|v_{r,s}\|_2^2. \quad (4.1)$$

If $0 \leq x, y < N$ then $|x \pm y\sqrt{d}| \leq N(1 + \sqrt{|d|}) \leq 2N\sqrt{q}$, and so each entry of the row $v_{r,s}$ is bounded in size by $R^J(2N\sqrt{q})^{r+s}$ where the R comes from the z -derivatives. Thus

$$\|v_{r,s}\|_2 \leq 2(N^2 J)^{1/2} R^J (2N\sqrt{q})^{r+s},$$

where the factor of 2 comes from the choice of $\langle, \rangle$. By Hadamard's inequality,

$$\begin{aligned} \log \det G &\leq RS \log(2N^2 J) + 2JRS \log R + RS(R + S) \log(2N\sqrt{q}) \\ &= R^2 S \left(\frac{1}{2} + O\left(\frac{1}{C}\right) \right) \log X + O(X^3), \end{aligned} \quad (4.2)$$

where for the last step we used the choice of parameters (2.1). This is the required upper bound.

5. p -ADIC BOUND

We now show that if $\chi(p) = -1$ then a large power of p divides $\det G$. Let e_p denote the exponent of the largest power of p dividing $\det G$.

Lemma 5.1. *Let p be an odd prime with $\chi(p) = -1$. Then*

$$e_p \geq 2 \sum_{\substack{0 \leq r < R \\ 0 \leq s < S}} \min\left(\left\lfloor \frac{r}{p} \right\rfloor, S - 1 - s\right).$$

Proof. Order the rows $v_{r,s}$ so that $(r', s') \prec (r, s)$ if $r' < r$; the precise order does not matter.

Now the key observation is that if $\psi(z, z') := z^p - z'$ then $\psi(P) \in p\mathbf{Z}[\sqrt{d}]$ for any $P = (x + y\sqrt{d}, x - y\sqrt{d})$, $x, y \in \mathbf{Z}$, and in particular for $P = P_i$. This is just the Frobenius relation that

$$(\sqrt{d})^p = d^{(p-1)/2} \sqrt{d} \equiv -\sqrt{d} \pmod{p\mathbf{Z}[\sqrt{d}]},$$

which implies that

$$(x + y\sqrt{d})^p \equiv x - y\sqrt{d} \pmod{p\mathbf{Z}[\sqrt{d}]}.$$

Fix, for now, r and s . Recall that the elements of row $v_{r,s}$ are $\partial_z^j(z^r(z')^s)|_{(z,z')=P_i}$, for $1 \leq i \leq N^2$ and $0 \leq j < J$. Set

$$h = h_{r,s} := \min\left(\left\lfloor \frac{r}{p} \right\rfloor, S - 1 - s\right). \quad (5.1)$$

We now consider the new row $\tilde{v}_{r,s}$ in which the entries are $\partial_z^j(z^{r-ph}\psi(z, z')^h(z')^s)|_{(z,z')=P_i}$.

We claim two things:

- (1) Every element of $\tilde{v}_{r,s}$ lies in $p^h\mathbf{Z}[\sqrt{d}]$;
- (2) $\tilde{v}_{r,s} = v_{r,s} +$ linear combination of $v_{r',s'}$ with $(r', s') \prec (r, s)$.

Item (1) follows from repeated applications of the product rule and the fact that $\psi(P_i) \in p\mathbf{Z}[\sqrt{d}]$, noting that all z -derivatives of ψ (of order at least 1) take values in $p\mathbf{Z}[\sqrt{d}]$ on all of $\mathbf{Z}[\sqrt{d}] \times \mathbf{Z}[\sqrt{d}]$.

For (2), first consider the case $j = 0$ where there is no derivative. Then by binomial expansion we have

$$z^{r-ph}(z^p - z')^h(z')^s = z^r(z')^s + \sum_{i=1}^h (-1)^i \binom{h}{i} z^{r-pi}(z')^{i+s}.$$

Thus (after considering derivatives) we in fact have

$$\tilde{v}_{r,s} = v_{r,s} + \sum_{i=1}^h (-1)^i \binom{h}{i} v_{r-pi, i+s}.$$

Note that, by the choice (5.1) of h , all the pairs $(r-pi, i+s)$ do lie in $\{0, 1, \dots, R-1\} \times \{0, 1, \dots, S-1\}$, and clearly $(r-pi, i+s) \prec (r, s)$. This establishes (2).

Let $\tilde{G}$ be the Gram matrix formed by the $\tilde{v}_{r,s}$. Due to the lower triangular nature of the relation (2), we have $\det \tilde{G} = \det G$.

By (1) and the definition of the Gram matrix, $p^{h+h'} \mid \tilde{G}_{(r,s),(r',s')}$, where $h = h_{r,s}$ and $h' := h_{r',s'}$, as defined in (5.1). We may extract a $p^{h_{r,s}}$ from the (r,s) -column of $\tilde{G}$, and $p^{h_{r',s'}}$ from the (r',s') -row, and thus obtain that $\det \tilde{G}$ is divisible by $p^{2\sum_{r,s} h_{r,s}}$. This concludes the proof. $\square$

6. COMPLETION OF THE PROOF

All that remains is to compare (4.1) with the information in Lemma 5.1. Since, in the notation of Lemma 5.1, we have $\log \det G = \sum_p e_p \log p$, we immediately obtain

$$2 \sum_{\substack{p \leq X \\ \chi(p)=-1}} \log p \sum_{r,s} \min\left(\left\lfloor \frac{r}{p} \right\rfloor, S - 1 - s\right) \leq R^2 S \left(\frac{1}{2} + O\left(\frac{1}{C}\right)\right) \log X + O(X^3). \quad (6.1)$$

By use of the inequality $\sum_{0 \leq s < S} \min(k, S - s - 1) \geq Sk - k^2$ (taking $k = \lfloor r/p \rfloor$ for each p) one can show that the LHS is

$$\geq 2S \sum_{\substack{p \leq X \\ \chi(p)=-1}} \log p \sum_{0 \leq r < R} \left\lfloor \frac{r}{p} \right\rfloor - O(X^3).$$

The error in replacing $\lfloor r/p \rfloor$ by r/p is $O(RS \sum_{p \leq X} \log p) = O(X^3)$, so this is

$$\geq 2S \sum_{\substack{p \leq X \\ \chi(p)=-1}} \log p \sum_{0 \leq r < R} \frac{r}{p} - O(X^3) = R^2 S \sum_{\substack{p \leq X \\ \chi(p)=-1}} \frac{\log p}{p} - O(X^3).$$

Comparing with (6.1) gives the bound claimed in Theorem 1.1.

APPENDIX A. RESULTANTS

We collect basic facts about resultants. First, let k be a field and let $f, g \in k[z]$ be polynomials in some indeterminate z , of degrees d, e respectively. Consider the map

$$\Phi : k[z]_{<e} \oplus k[z]_{<d} \rightarrow k[z]_{<d+e}$$

given by $\Phi(P, Q) := fP + gQ$. The matrix of this linear map with respect to the descending monomial bases of the respective vector spaces (that is,

$$\{(z^{e-1}, 0), \dots, (z, 0), (1, 0), (0, z^{d-1}), (0, z^{d-2}), \dots, (0, 1)\}$$

on the left, and $\{z^{d+e-1}, z^{d+e-2}, \dots, 1\}$ on the right) is called the *Sylvester matrix*, and its determinant is defined to be $\text{Res}_z(f, g)$; this is just an element of k . A well-known fact is that $\text{Res}_z(f, g) = 0$ if and only if f, g have a non-constant common factor.

In the main part of the note we apply this construction with $k = \mathbf{C}(z')$, with $f \in \mathbf{C}[z, z'] \subset k[z]$ some irreducible polynomial with degree (d, d') , $d > 0$, and with $g = \partial_z f$. Consider the resultant $\text{Res}_z(f, \partial_z f)$. By construction, this is a polynomial in z' , and it is non-zero since f is irreducible, and hence has no common factor with $\partial_z f$.

$\text{Res}_z(f, \partial_z f)$ is given by a $(2d-1) \times (2d-1)$ determinant, each of whose entries is a polynomial in z' of degree $\leq d'$, so (crudely)

$$\deg_{z'} \text{Res}_z(f, \partial_z f) \leq 2dd'. \quad (\text{A.1})$$

Now we prove the key fact used in the main text, (3.5).

Lemma A.1. *With the setup as above, suppose that for some fixed z'_0 we have that $f(z, z'_0)$ is not identically zero, and has a root of multiplicity $\mu \geq 1$ at some $z = z_0$. Then*

$$\text{ord}_{z=z_0} f(z, z'_0) \leq 1 + \text{ord}_{z'=z'_0} \text{Res}_z(f, \partial_z f).$$

Proof. The assumption implies that both $f(z, z'_0)$ and $\partial_z f(z, z'_0)$ are divisible by $(z - z_0)^{\mu-1}$, and so every polynomial in $\text{im } \Phi$ is divisible by $(z - z_0)^{\mu-1}$ when we specialize to $z' = z'_0$. Therefore, $\dim \text{im } \Phi|_{z'=z'_0} \leq (2d-1) - (\mu-1) = 2d - \mu$.

Thus, if we write $S(z')$ for the Sylvester matrix, $\text{rk}(S(z'_0)) \leq 2d - \mu$. Therefore there are $\mu - 1$ linearly independent vectors $u_1, \dots, u_{\mu-1} \in \mathbf{C}^{2d-1}$ such that $u_i^T S(z'_0) = 0$. Complete to a basis $u_1, \dots, u_{2d-1}$ of $\mathbf{C}^{2d-1}$, and let U be the matrix formed from the u_i^T . Thus the first $\mu - 1$ rows of $US(z'_0)$ are zero. Consider now $US(z')$, which is a matrix whose entries are polynomials in z' . By what we just said, the first $\mu - 1$ rows of $US(z')$ are divisible by $z' - z'_0$, and so $\det(US(z'))$ is divisible by $(z' - z'_0)^{\mu-1}$. Since $\text{Res}_z(f, \partial_z f) = \det S(z') = (\det U)^{-1} \det(US(z'))$, we have $\text{ord}_{z'=z'_0} \text{Res}_z(f, \partial_z f) \geq \mu - 1$ and the result follows. $\square$

REFERENCES

- [1] W. D. Banks, *On the OpenAI proof that Landau–Siegel zeros do not exist*, arXiv:2610.15483.
- [2] B. Kerr, *A simpler proof that there are no Landau–Siegel zeros*, arXiv:2610.21099.
- [3] OpenAI, *Uniform exclusion of Landau–Siegel zeros*, OpenAI Math Release preprint (2026). [Available online](#).
Email address: `ben.green@maths.ox.ac.uk`