STEPANOV WITHOUT MULTIPLICITY: A DETERMINANT AGAINST SIEGEL ZEROS

Prerequisites. Fermat's little theorem, Euler's criterion, Legendre's formula for $\operatorname{ord}_p n!$, Stirling's formula, the Euler–Maclaurin formula, Mertens' estimate $\sum_{p\le x}\log p/p = \log x + O(1)$, and Chebyshev's bound $\theta(N) := \sum_{p\le N}\log p \le N\log 4$. Quadratic fields and the Kronecker symbol χ_D; every primitive real character is a χ_D [Dav, Ch. 5]. Section 7.2 uses Section 5.2 of Chapter 5. We follow [N, §§2–8, App. D]. Section 7.4 uses the function G of (1) in Chapter 1. Sections 7.4–7.5 point ahead to Sections 8.1–8.5 of the next chapter, Chapter 8, but use nothing from it.

7.1. Chebyshev's determinant

How much can the size and divisibility of one integer say about primes? For $N \ge 2$ let $V_N := \det(u^a)_{1\le u\le N,\,0\le a<N} = \prod_{1\le i<j\le N}(j-i)$.

Problem 7.1.1. $V_N = \prod_{a<N} a!$, and $\log V_N \le \frac{1}{2}N(N-1)\log N$.

Problem 7.1.2. $\operatorname{ord}_p V_N \ge \sum_{a<N}\lfloor a/p\rfloor \ge N^2/(2p) - N/2$. For $N = 4$, $p = 2$ the first inequality is an equality.

Problem 7.1.3. $\sum_{p\le N}\log p/p \le \log N + 2$.

Each prime is seen through the single congruence $u^p \equiv u \pmod p$, once for each complete block of p exponents. This proof is given in [N, App. A], which credits the observation to Pascadi and to Tao [Tao].

7.2. The Frobenius graph

Let D be a fundamental discriminant, $F := \mathbb{Q}(\sqrt{D}) \subset \mathbb{C}$, σ the nontrivial automorphism, and $\mathcal{O}_F = \mathbb{Z}[\omega]$ with $\omega = (1+\sqrt{D})/2$ or $\sqrt{D}/2$. We want $\sum_{p\le t,\,\chi_D(p)=-1}\log p/p \le (\frac{1}{2}+o(1))\log t$.

Problem 7.2.1. If p is odd and $\chi_D(p) = -1$, then $u^p \equiv \sigma(u) \pmod{p\mathcal{O}_F}$ for all $u \in \mathcal{O}_F$. For instance, $(1+i)^3 \equiv 1-i \pmod 3$.

So modulo such p the points $(u,\sigma(u))$ lie on the graph $Y = X^p$. This is all that Section 5.2 of Chapter 5 used about $\mathbb{Z}[i]$, and we now run that section with $\mathbb{Z}[i]$, $\bar{u}$ and the primes $p \equiv 3 \pmod 4$ replaced by $\mathcal{O}_F$, $\sigma(u)$ and the odd primes p with $\chi_D(p) = -1$. For integers $t \ge 2$, $H \ge 1$ let $\mathcal{T} := \{(a,b) \in \mathbb{Z}^2_{\ge 0} : a + Hb < t\}$, $T := |\mathcal{T}|$, $A := \sum_{\mathcal{T}} a$.

Problem 7.2.2. Problem 5.2.2 holds in this setting: if p is odd, $\chi_D(p) = -1$, $f \in \mathcal{O}_F[X,Y]$ and $u \in \mathcal{O}_F$, then $\big(\partial_X^j((X^p-Y)^k f)\big)(u,\sigma(u)) \in p^k\mathcal{O}_F$ for all $j,k \ge 0$.

Let $u_1,\dots,u_I \in \mathcal{O}_F$, $J \ge 1$, and let M be the $IJ \times T$ matrix with entries $(\partial_X^j X^a Y^b)(u_i,\sigma(u_i))$, $0 \le j < J$. Let P_H be the set of odd $p \ge H$ with $\chi_D(p) = -1$, and $k_p := \sum_{\mathcal{T}}\lfloor a/p\rfloor$.

Date: November 25, 2026.

Problem 7.2.3. For $p \in P_H$, the set $\mathcal{T}$ satisfies the hypothesis of Problem 5.2.3, and every $T \times T$ minor of M lies in $p^{k_p}\mathcal{O}_F$.

Problem 7.2.4. Let $|u_i|, |\sigma(u_i)| \le B$ with $B \ge 1$, and let δ be a nonzero $T \times T$ minor. Then $\delta\sigma(\delta)$ is a nonzero integer divisible by p^{2k_p} for $p \in P_H$, and $|\delta|, |\sigma(\delta)| \le T^T t^{T(J-1)} B^{\sum_{\mathcal{T}}(a+b)}$.

Problems 7.2.1–7.2.4 prove the following, which for $\mathbb{Z}[i]$ also follows from Theorem 5.2.1.

Theorem 7.2.1. *If $|u_i|, |\sigma(u_i)| \le B$, $B \ge 1$, and M has rank T, then*

$$\sum_{p \in P_H} k_p \log p \le \Big(\sum_{\mathcal{T}} (a+b)\Big) \log B + T \log T + T(J-1)\log t. \tag{1}$$

Problem 7.2.5. If $I \ge |D|$, there are I distinct $u \in \mathcal{O}_F$ with $|u|, |\sigma(u)| \le 4I^{1/2}|D|^{1/4}$.

7.3. Density one half

Without derivatives, (1) gives nothing in a quadratic field [N, Ex. 24].

Problem 7.3.1. Distinct $u_i \in \mathcal{O}_F$ with $|u_i|, |\sigma(u_i)| \le B$ number at most $25B^2$. Hence if $J = 1$ and M has rank T, then $\log B \ge \log t - \frac{1}{2}\log H - 3$.

So for $J = 1$ the bound from (1) for $\sum_{H \le p \le t,\, \chi_D(p) = -1} \log p/p$ is at least $\log t - \frac{1}{2}\log H - 3$, worse than Mertens' $\log(t/H) + O(1)$. Derivatives let I be about T/J [Gr]. The interpolation input, by a Wronskian argument that [Ko, proof of Thm. 1] and [N, Lemma 17] credit to Barreto: if the u_i are distinct, $I = 2t$ and $J = 2\lfloor (t-1)/H \rfloor + 1$, then M has rank T. For $t \ge 6$, $1 \le H \le t/2$ one has $T \le t^2/H$, $A \ge t^3/(8H)$ and $\sum_{\mathcal{T}} b \le 8A/H$.

Problem 7.3.2. Under the hypotheses of Theorem 7.2.1, with $t \ge 6$ and $H \le t/2$, $\sum_{p \in P_H,\, p \le t} \log p/p \le (1 + 8/H)\log B + (8/t)\big(\log T + (J-1)\log t\big) + 16$.

Problem 7.3.3. For $t \ge \max(16, |D|/2)$, $H = \lceil \log t \rceil$, $I = 2t$, $J = 2\lfloor (t-1)/H \rfloor + 1$ and the points of Problem 7.2.5,

$$\sum_{p \le t,\ \chi_D(p) = -1} \frac{\log p}{p} \le \frac{1}{2}\log t + \frac{1}{4}\log|D| + \log\log(3t) + 50.$$

A primitive real χ of conductor q has no real zero in $(1 - c/\log 2q, 1)$, with c effective and depending only on κ, B_0, provided $\sum_{p \le x,\, \chi(p) = -1} \log p/p \le \kappa \log x + B_0 \log 2q$ for all $x \ge 2$ and some $\kappa < 1$ [N, Lemma 2, App. F].

Problem 7.3.4. Problems 7.1.3 and 7.3.3 give this with $\kappa = \frac{3}{4}$, $B_0 = 30$.

Thus we have proved the following.

Theorem 7.3.1. *There is an effective absolute $c > 0$ such that $L(s, \chi) \ne 0$ for real $s > 1 - c/\log(2q)$, for every primitive real character χ of conductor q.*

This was first proved in [OAI], with three variables in a biquadratic field; the proof here follows [Gr] and [N].

7.4. One congruence per block

Alpöge called this argument "Stepanov without multiplicity" [Alp, p. 2]. What does it lose? For V_N both sides are exact. Let r_n be the remainder of N modulo n, and $W(N) := \sum_{n \le N} \Lambda(n)\, r_n(n - r_n)/(2n)$.

Problem 7.4.1. $\sum_{a<N} \lfloor a/n \rfloor = \frac{N}{2}\big(\frac{N}{n} - 1\big) + \frac{r_n(n-r_n)}{2n}$. Hence $\log V_N = \frac{N}{2} \sum_{n \le N} \Lambda(n) \big(\frac{N}{n} - 1\big) + W(N)$, with $0 \le W(N) \le N\psi(N)/8$, where $\psi(N) := \sum_{n \le N} \Lambda(n)$.

Problem 7.4.2. For G as in (1) of Chapter 1, $G(N) = (\gamma - \frac{1}{2})N - 2W(N)/N + O(1)$. In particular $G(N) \le (\gamma - \frac{1}{2})N + O(1)$.

For $N = 10^4$, $G(N) = 1.749\ldots$ while $(\gamma - \frac{1}{2})N = 772.15\ldots$. The determinant gives a one-sided bound for G with error of order N, and nothing more: the rest is the sawtooth sum $W(N)$. In Section 7.2 the floors $\lfloor a/p \rfloor$ cost the constant 16 of Problem 7.3.2 in the same way. An error $O(1)$ in $\sum \log p/p$ is Chebyshev strength. It suffices for Theorem 7.3.1, where a real zero would change the main term by a constant factor. It is far from $G(x) \le x^{1/2+\varepsilon}$, which the Riemann hypothesis needs. One determinant is a chain of length $m = 1$ in Problem 8.5.1.

7.5. Multiplicity in Bombieri's form

Stepanov's polynomial vanishes to order about $\sqrt{q}$ (Theorem 8.3.1); order one gives nothing (Problem 8.1.4). Bombieri gets multiplicity from a power of Frobenius [Bom74], [N, App. D].

Let k be a finite field of odd characteristic, $f \in k[X]$ of degree $d = 2g + 1$, $g \ge 1$, and $R := k[x, y]$ with $y^2 = f(x)$. For $\phi = a(x) + b(x)y$ let $\lambda(\phi) := \deg(a^2 - b^2 f)$, and $R_\ell := \{\phi : \lambda(\phi) \le \ell\}$.

Problem 7.5.1. $\lambda(a + by) = \max(2 \deg a, 2 \deg b + d)$ and $\lambda(\phi\psi) = \lambda(\phi) + \lambda(\psi)$; $\dim_k R_\ell = \ell + 1 - g$ for $\ell \ge 2g$.

Problem 7.5.2. A nonzero $\phi \in R$ vanishes at no more than $\lambda(\phi)$ points (ξ, η) over a finite extension of k.

Let Q be a power of $|k|$, and N the number of $(\xi, \eta) \in \mathbb{F}_{Q^2}^2$ with $\eta^2 = f(\xi)$. Let $2g \le \ell_1 < Q$, $\ell_2 \ge 2g$, and (x_i), (y_j) bases of R_{ℓ_1}, R_{ℓ_2} with distinct λ. For $c_{ij} \in k$ let $f_c := \sum c_{ij} x_i y_j^Q$ and $\tilde{f}_c := \sum c_{ij} x_i^Q y_j$.

Problem 7.5.3. If $c \ne 0$ and $\tilde{f}_c = 0$, then $f_c \ne 0$, f_c vanishes at all N points, and $N \le \ell_1 + Q\ell_2$.

Problem 7.5.4. Such c exists for $\ell_1 = Q - 1$, $\ell_2 = Q + 2g$ if $Q > (g + 1)^2$. Hence $N \le Q^2 + (2g + 1)Q - 1$.

For $f = X^3 - X$ over $\mathbb{F}_3$ and $Q = 27$, $N = 783$ and the bound is 809. The function f_c^Q vanishes to order at least Q at each of these points, for free, because $(\sum c\phi)^Q = \sum c^Q \phi^Q$, $c^Q = c$, and all points share the Frobenius $\xi \mapsto \xi^{Q^2}$.

Problem 7.5.5. $(X+Y)^p - X^p - Y^p \in p\mathbb{Z}[X, Y] \setminus p^2\mathbb{Z}[X, Y]$. The primes $p < 4000$ with $2^p \equiv 2 \pmod{p^2}$ are 1093 and 3511.

Over $\mathbb{Z}$ the p-th power is additive and fixes integers only modulo p, and p varies. The determinant of Section 7.2 is nonzero by interpolation, handles all $p \geq H$ because $\mathcal{T}$ is stable under $X^p \mapsto Y$, and sees p because $X^p - Y$ vanishes at $(u, \sigma u)$ to first order modulo p. In the proof the multiplicity returns through a chain of m maps (Theorem 8.4.1 of the next chapter), and the budget $x/m+m$ of Problem 8.5.2 balances at $m \approx \sqrt{x}$, as ℓ and Q do above.

Hints

§7.1.

7.1.2: Use $u^p \equiv u \pmod p$ to change the columns by a unitriangular matrix. For the second inequality, split $[0, N)$ into blocks of length p.

7.1.3: Sum Problem 7.1.2 over $p \leq N$ with weight $\log p$, and use Chebyshev's bound.

§7.2.

7.2.1: Write $2u = x + y\sqrt{D}$ and use Euler's criterion for $D^{(p-1)/2}$.

7.2.2: Problem 7.2.1 and the Leibniz rule, as for Problem 5.2.2.

7.2.3: $p \geq H$. Then the proof of Problem 5.2.3, with Problem 7.2.2.

7.2.5: Take $x + y\omega$ in a box with $|x| \approx |y|\sqrt{|D|}$; note $|\omega|, |\sigma\omega| \leq \sqrt{|D|}$.

§7.3.

7.3.1: Count the possible values of $u + \sigma u$ and $(u - \sigma u)/\sqrt{D}$. For the second claim compare T with I.

7.3.2: $\lfloor a/p \rfloor \geq a/p - 1$, and $\theta(t) \leq 2t$.

7.3.3: Insert Problem 7.2.5 into Problem 7.3.2, and treat the primes below H by Problem 7.1.3.

7.3.4: Absorb $\log\log(3t)$ into $\frac{1}{4}\log t$ plus a constant.

§7.4.

7.4.1: Split $[0, N)$ into blocks of length n. Then $\log a! = \sum_n \Lambda(n)\lfloor a/n \rfloor$.

7.4.2: Show $\frac{2}{N}\log V_N = N\log N - \frac{3}{2}N + O(1)$ by Stirling and Euler–Maclaurin.

§7.5.

7.5.1: Parity of $2\deg a$ and $2\deg b + d$; $a^2 - b^2 f$ is ϕ times its conjugate.

7.5.2: Count the roots of $a^2 - b^2 f$ with multiplicity.

7.5.3: The $\lambda(x_i y_j^Q)$ are distinct. At the points, $f_c^Q = \sum c\, x_i^Q y_j^{Q^2}$ takes the value of $\tilde{f}_c$.

7.5.4: $\tilde{f}_c \in R_{Q\ell_1+\ell_2}$; compare dimensions.

7.5.5: The coefficient of $X^{p-1}Y$ is p.

References

[Alp] L. Alpöge, untitled note announcing a proof of the Riemann hypothesis, 20 November 2026, `https://alpo.ge/remark.pdf`.

[Bom74] E. Bombieri, *Counting points on curves over finite fields (d'après S. A. Stepanov)*, Séminaire Bourbaki, Exp. 430, Lecture Notes in Math. **383**, Springer, 1974, 234–241.

[Dav] H. Davenport, *Multiplicative Number Theory*, 3rd ed., revised by H. L. Montgomery, Grad. Texts in Math. **74**, Springer, 2000.

[Gr] B. Green, *On Landau–Siegel zeros*, Hexagon preprint hexagon:2610.00311v2, 2026, `https://hexagonmath.org/2610.00311v2`.

[Ko] S. D. Kominers, *Small algebraic integers and Frobenius prime sums*, Hexagon preprint hexagon:2610.00451v1, 2026, https://hexagonmath.org/2610.00451v1.

[N] P. D. Nelson, *Some notes on recent results on Landau–Siegel zeros*, note, 2026, https://ultronozm.github.io/math/20261020T163023--siegel-zeros.html.

[OAI] OpenAI, *Uniform exclusion of Landau–Siegel zeros*, OpenAI Math Release preprint, 1 October 2026, https://github.com/openai/math/blob/main/preprints/Uniform-exclusion-of-Landau-Siegel-zeros-October-1-2026/paper.pdf.

[Tao] T. Tao, *A sketch of the proof of non-existence of Siegel zeroes*, What's new, 19 October 2026, https://terrytao.wordpress.com/2026/10/19/a-sketch-of-the-proof-of-non-existence-of-siegel-zeroes/.