

A proof Gauss might have found

Roelof van Dijk

Abstract

Ben Green's historical variant of Tao's recent tenth discriminant challenge [5] asks how early Gauss's class-number-one conjecture could have been proved using mathematics then in print. Through discussions with GPT-6 Astra and Opus 5.5, we construct a proof of Gauss's class-number-one conjecture [1] from ingredients published by 1808, specializing the Frobenius determinant argument [6]. Counting values of the principal form and summing factorial valuations reduce the proof to a residue sieve below 17000.

Theorem. *The negative fundamental discriminants of class number one are*

$$-3, -4, -7, -8, -11, -19, -43, -67, -163.$$

Proof. Write the discriminant as $-q$ and suppose $h(-q) = 1$.

The principal form [1] is $f = (x + y/2)^2 + qy^2/4$ if $q \equiv 3 \pmod{4}$ and $f = x^2 + qy^2/4$ if $4 \mid q$. Its values are squares or at least $q/4$. Call a prime ℓ inert if $b^2 \equiv -q \pmod{4\ell}$ has no solution. Otherwise $(\ell, b, \frac{b^2+q}{4\ell})$ is primitive, since $-q$ is fundamental, and is equivalent to f . Thus every non-inert prime is a value $f(u, v)$ with $v \neq 0$, and is at least $q/4$. In particular,

$$\text{every prime } \ell < q/4 \text{ is inert.} \quad (1)$$

Assume $q > 8$. Inertness of 2 gives $q \equiv 3 \pmod{8}$. Then q is odd and squarefree, and must be prime: a composite odd squarefree integer has a prime factor below $q/4$, whereas every prime factor of q is non-inert.

Put $\omega = (1 + \sqrt{-q})/2$ and $O = \mathbb{Z}[\omega]$, with $\omega^2 = \omega - (q+1)/4$. Write $\bar{z}$ for the conjugate of z . For every inert prime ℓ and $z \in O$,

$$z^\ell \equiv \bar{z} \pmod{\ell O}. \quad (2)$$

Indeed $(a + b\omega)^\ell \equiv a + b\omega^\ell$ by the binomial theorem and Fermat. For odd ℓ , Euler's criterion gives $(2\omega)^\ell \equiv 1 - \sqrt{-q} = 2\bar{\omega}$. Since $2^\ell \equiv 2$ and ℓ is odd, $\omega^\ell \equiv \bar{\omega}$. At $\ell = 2$, the integer $(q+1)/4$ is odd, so $\omega^2 \equiv \omega + 1 \equiv \bar{\omega}$. For an odd inert p , the identity $4(a^2 + ab + \frac{q+1}{4}b^2) = (2a + b)^2 + qb^2$ shows that the norm of $a + b\omega$ is prime to p unless $p \mid a, b$. Thus O/pO is a field, with inverses $\bar{z}/(z\bar{z})$, in which $z^p = \bar{z}$.

We use (2) twice: first to prove a determinant nonzero modulo a large inert prime, then to give it too many prime factors for its size. For an inert prime p , the determinant will have order pS , where $S = \lfloor p/40 \rfloor$. After division by $S p^2$, the logarithm of its norm will be at least $\log p$ minus an absolute constant, and at most $\frac{21}{40} \log p + \frac{1}{4} \log q$. Choosing $q^3/(5 \log q) < p \leq q^3$ makes the difference grow like $\frac{47}{40} \log q$. The principal-form count supplies p and bounds the contribution of the non-inert primes.

Suppose $q \geq 17000$, and let $N(x)$ count the non-inert primes at most x . Choose their representations with $v > 0$ and $u + v/2 \geq 0$. For $x > 0$,

$$N(x) \leq \sum_{1 \leq v \leq 2\sqrt{x/q}} \left(\sqrt{x - qv^2/4} + 1 \right) \leq \frac{5x}{3\sqrt{q}} + 2\sqrt{\frac{x}{q}}.$$

The last inequality follows from $\sqrt{1 - t^2} \leq 1 - t^2/2$ and comparison with an integral. For $\ell \leq Y = q^3$,

$$\frac{\log \ell}{\ell} = \frac{\log Y}{Y} + \int_{\ell}^Y \frac{\log t - 1}{t^2} dt.$$

Adding over the non-inert primes and using $N(t) = 0$ for $t \leq q/4$ gives

$$\sum_{\substack{\ell \leq q^3 \\ \ell \text{ not inert}}} \frac{\log \ell}{\ell} \leq \frac{5}{6\sqrt{q}} (8 \log^2 q + 5 \log q) + \frac{8 \log q + 8}{q} < 5.2. \quad (3)$$

The bound decreases for $q \geq 17000$. At 17000, use $\log q < 9.75$ and $\sqrt{q} > 130$.

Let $n = \lfloor q^3/2 \rfloor$. Legendre's formula [2, Introduction, art. XVI, pp. 8–9] gives $v_\ell \binom{2n}{n} \leq \log(2n)/\log \ell$: each summand $\lfloor 2n/\ell^j \rfloor - 2\lfloor n/\ell^j \rfloor$ is 0 or 1, and vanishes for $\ell^j > 2n$. Thus every prime power exactly dividing $\binom{2n}{n}$ is at most $2n$. There are at most $X/2 + 1$ primes up to $X = q^3/(5 \log q)$. If all the inert prime divisors of $\binom{2n}{n}$ were at most X , then

$$4^n/(2n+1) \leq \binom{2n}{n} \leq (2n)^{X/2+1+N(2n)}.$$

The logarithms of the two bounds are greater than $0.69q^3$ and less than $0.68q^3$, respectively. Hence there is an inert prime p with

$$q^3/(5 \log q) < p \leq q^3, \quad p > 10^{11}.$$

Put

$$m = \left\lceil \sqrt{\frac{p}{2\sqrt{q}}} \right\rceil, \quad B = m\sqrt{q/2}.$$

The elements $a + b\omega$ with $|b| \leq m$ and $|2a + b| \leq m\sqrt{q}$ number at least $(2m+1)\lfloor m\sqrt{q} \rfloor \geq 2\sqrt{q}m^2 \geq p$, and have absolute value at most B . The difference of two of them has norm at most $4B^2 < p^2$, so they are distinct modulo p . Choose p of them, $z_1, \dots, z_p$. Then

$$\log B \leq \frac{1}{2} \log p + \frac{1}{4} \log q - \log 2 + 0.001. \quad (4)$$

Match the S successive y -degrees with the S derivative orders in x . The degrees provide room for factors $x^\ell - y$, while the derivatives cancel the added powers of B . Form the square matrix A with rows (r, s) , $0 \leq r < p$, $0 \leq s < S$, columns (i, j) , $1 \leq i \leq p$, $0 \leq j < S$, and entries

$$A_{(r,s),(i,j)} = \partial_x^j (x^r y^s) \big|_{(x,y)=(z_i, \bar{z}_i)} \in \mathcal{O}.$$

These are ordinary derivatives. Dividing the ℓ th derivative of x^ℓ by $\ell!$ would lose the factor ℓ needed below. A relation between the rows modulo p , with coefficients c_{rs} , gives the polynomial $G(x) = \sum c_{rs} x^{r+ps}$. Since $\bar{z}_i = z_i^p$ and $(x^{ps})' = 0$ in characteristic p , we have $G^{(j)}(z_i) = 0$ for $j < S$. As $S < p$, the p distinct roots z_i each have multiplicity at least S . But $\deg G < pS$, so $G = 0$. The exponents $r + ps$ are distinct, hence every c_{rs} is zero. Thus $\Delta = \det A \neq 0$ modulo p , and $D = \Delta \bar{\Delta}$ is a positive integer.

Each entry has absolute value at most $p^j B^{r+s-j}$. The derivative orders cancel the s -degrees:

$$\sum_{i,j} j = \sum_{r,s} s = \frac{pS(S-1)}{2}.$$

The Leibniz expansion therefore gives

$$\begin{aligned} \log D &\leq 2 \log((pS)!) + pS(p-1) \log B + pS(S-1) \log p \\ &\leq Sp^2(\log B + \frac{1}{40} \log p + 10^{-6}), \end{aligned}$$

since $S \leq p/40$ and $4 \log p/p < 10^{-6}$.

Fix an inert prime $\ell < p$. Replace row (r, s) by the row of $x^{r-\ell h} (x^\ell - y)^h y^s$, where $h = \min(\lfloor r/\ell \rfloor, S-1-s)$. The added monomials have smaller x -degree and y -degree below S . Ordered by x -degree, the change of basis is triangular with diagonal entries one, so Δ is unchanged. By (2) and Leibniz's rule each new entry lies in $\ell^h \mathcal{O}$, because $z_i^\ell - \bar{z}_i \in \ell \mathcal{O}$ and every positive derivative of x^ℓ has coefficient divisible by ℓ . Factoring ℓ^h from each row gives $\Delta \in \ell^{\sum_{r,s} h} \mathcal{O}$, hence $\ell^{2 \sum_{r,s} h} \mid D$, and these integer divisibilities multiply over distinct primes. For every prime ℓ , put

$$E_\ell = \sum_{r < p, s < S} \min(\lfloor r/\ell \rfloor, S-1-s) = \sum_{k \geq 1} (S-k)_+ (p-k\ell)_+,$$

where $x_+ = \max(x, 0)$. Put $\alpha = p/S$. The corresponding integral is $\int_0^\infty (S-t)_+(p-\ell t)_+ dt = Sp^2 w_\alpha(\ell)/2$, where

$$w_\alpha(t) = \frac{1}{\max(\alpha, t)} - \frac{\min(\alpha, t)}{3 \max(\alpha, t)^2}.$$

Write $T_\ell = \sum_{r < p} \lfloor r/\ell \rfloor$, $V_\ell = \sum_{r < p} v_\ell(r!)$ and $L = \sum_{r < p} \log r!$. Lemma 1 gives $E_\ell \geq (S\ell w_\alpha(\ell) - 1)T_\ell$. Together with Legendre's bounds

$$(\ell - 1)V_\ell \leq \ell T_\ell, \quad T_\ell \leq V_\ell \leq \frac{p^2}{2(\ell - 1)},$$

and $0 \leq \ell w_\alpha(\ell) \leq 1$, this yields

$$E_\ell \geq (S - 1)V_\ell - \frac{Sp^2}{2} \left(\frac{1}{\ell - 1} - w_\alpha(\ell) \right).$$

Since $\sum_\ell V_\ell \log \ell = L$, summing over primes gives

$$\sum_\ell E_\ell \log \ell \geq (S - 1)L - \frac{Sp^2}{2} C_p(\alpha), \quad C_p(\alpha) = \sum_{\substack{\ell \leq p \\ \ell \text{ prime}}} \log \ell \left(\frac{1}{\ell - 1} - w_\alpha(\ell) \right).$$

All prime sums here are restricted to $\ell \leq p$. Lemma 1 also gives $C_p(\alpha) < 3.5$, since $40 \leq \alpha < 40.001$ and $\log \alpha < 3.69$. Removing the non-inert primes costs at most $5.2Sp^2/2$, by (3) and $E_\ell \leq ST_\ell \leq Sp^2/(2\ell)$. Using $L \geq \frac{p^2}{2}(\log p - \frac{3}{2}) - p \log p$, we obtain

$$\log D \geq Sp^2(\log p - 10.21), \quad (5)$$

where $2 \log p/p + \log p/S < 0.01$ covers the discrete error.

Comparing the two bounds for $\log D$, and using (4) and $p > q^3/(5 \log q)$, gives

$$\frac{47}{40} \log q - \frac{19}{40} \log(5 \log q) < 9.52.$$

The left side increases with q . At $q = 17000$, it exceeds

$$\frac{47}{40}(9.74) - \frac{19}{40}(3.89) = 9.59675 > 9.52.$$

Thus $q < 17000$.

It remains to use (1) below 17000. For $q > 124$, the tests at 3 and 5 give $q = 120k + a$ with $a = 43$ or 67 and $0 \leq k < 142$. The tests at 7, 11, 13, 17, 31 give

a	$k \pmod{7}$	$k \pmod{11}$	k
43	0, 1, 3	1, 5, 6, 7, 9	1, 49, 122
67	0, 4, 5	0, 3, 7, 8, 9	117

To obtain the last column, combine residues u modulo 7 and v modulo 11 by $k \equiv 22u - 21v \pmod{77}$, then apply the tests at 13, 17, 31. This leaves $q = 163, 5923, 14683, 14107$. For the last three, respectively, $-q \equiv 14^2, 7^2, 4^2 \pmod{29}$, contradicting (1). For $8 < q \leq 124$, the applicable tests at 3 and 5 leave 11, 19, 43, 67. The fundamental discriminants with $q \leq 8$ are $-3, -4, -7, -8$. For each of the nine surviving discriminants, Gauss reduction [1, arts. 171–175] $|b| \leq a \leq c$, $3a^2 \leq q$ leaves only the principal form. $\square$

Lemma 1 (Row weights). *Let p, S be positive integers with $\alpha = p/S \geq 4$, and define E_ℓ, T_ℓ, w_α and $C_p(\alpha)$ as above. For every prime ℓ ,*

$$E_\ell \geq (S\ell w_\alpha(\ell) - 1)T_\ell, \quad C_p(\alpha) \leq \frac{\log^2 \alpha - \log \alpha + 11}{6}.$$

Proof. Put $u = p/\ell$, $H = \sum_{k \geq 1} (u - k)_+$ and $F = \sum_{k \geq 1} (S - k)_+ (u - k)_+$. Then $T_\ell = \ell H$ and $E_\ell = \ell F$. The claim is immediate if $H = 0$. For $u \geq S$, direct summation and $H \leq u^2/2$ give

$$F = \frac{S(S-1)}{2} \left(u - \frac{S+1}{3} \right), \quad \frac{F}{H} \geq \frac{S^2}{u} - \frac{S^3}{3u^2} - 1,$$

the difference in the latter inequality being at least $1 - S/u + S/(3u^2) \geq 0$. For $u \leq S$, write $J = \sum_{k \geq 1} k(u-k)_+$ and $n = \lfloor u \rfloor$. The bound $F/H \geq S - u/3 - 1$ follows from

$$F = SH - J, \quad (u+2)H - 3J = n \left((u-n)^2 + \frac{n-1}{2} \right) \geq 0.$$

For the second, put $f(t) = \log t((t-1)^{-1} - w_\alpha(t))$. This is nonnegative and convex for $t \geq 2$. On $t \leq \alpha$, write $f(t) = \log t/(t-1) - \log t/\alpha + t \log t/(3\alpha^2)$ and use

$$\frac{\log t}{t-1} = \int_0^1 \frac{dv}{1+v(t-1)}.$$

On $t \geq \alpha$, write $f(t) = \log t/[t(t-1)] + (\alpha/3) \log t/t^2$. The first term is a product of positive decreasing convex functions, and the second has nonnegative second derivative. The values and first derivatives agree at $t = \alpha$. For $c = 6j+5$ or $6j+7$, integrate $f(c-u) + f(c+u) \geq 2f(c)$ over $0 \leq u \leq 3$. Every prime beyond 3 has one of these forms, so

$$C_p(\alpha) \leq f(2) + f(3) + \frac{1}{6} \int_2^\infty f(t) dt + \frac{1}{6} \int_4^\infty f(t) dt.$$

For $2 \leq b \leq \alpha$, direct integration gives

$$\begin{aligned} \int_b^\infty f(t) dt &= \frac{\log^2 \alpha - \log^2 b - \log \alpha}{2} + \frac{5}{4} + \int_b^\infty \frac{\log t}{t(t-1)} dt \\ &\quad + \frac{b}{\alpha} (\log b - 1) + \frac{b^2}{12\alpha^2} (1 - 2 \log b). \end{aligned}$$

The remaining integral is at most

$$\int_b^\infty \frac{\log t}{(t-1)^2} dt = \frac{\log b}{b-1} + \log \frac{b}{b-1}.$$

Substituting $b = 2, 4$ and collecting terms yields

$$C_p(\alpha) \leq \frac{\log^2 \alpha - \log \alpha}{6} + \frac{16}{9} \log 2 + \frac{1}{3} \log 3 + \frac{5}{12} (1 - (\log 2)^2) - \frac{1}{\alpha} + \frac{2}{\alpha^2}.$$

Here we used $0.69 < \log 2 < 0.70$ and $1 < \log 3 < 1.1$ to bound the coefficients of α^{-1} and α^{-2} by -1 and 2 . The same bounds make the constant terms less than $11/6$, while $-1/\alpha + 2/\alpha^2 \leq 0$. $\square$

Gauss writes forms as $ax^2 + 2bxy + cy^2$ [1, art. 153]. Our form (a, b, c) corresponds to his improperly primitive form $(2a, b, 2c)$ when b is odd, and to his properly primitive form $(a, b/2, c)$ when b is even [1, art. 226]. Arithmetic in $\mathcal{O}$ is arithmetic on pairs of integers, with the displayed multiplication rule. Modulo p , the inversion formula supplies everything needed for the polynomial root count. The weighted prime sum uses only integration and finite addition. Determinant expansion and row operations appear in Laplace [3, §IV]. Legendre's factorial formula appears in [2, Introduction, art. XVI].

When the class number is one, the principal form represents every non-inert prime. Lattice counting and factorial valuations then force a large inert prime divisor of the central binomial coefficient, by a comparison similar to Chebyshev's later work [4].

References

- [1] C. F. Gauss, *Disquisitiones arithmeticae*, Leipzig, 1801. <https://doi.org/10.3931/e-rara-4025>.
- [2] A.-M. Legendre, *Essai sur la théorie des nombres*, second edition, Paris, 1808, Introduction, art. XVI, pp. 8–9. https://archive.org/details/bub_gb_BwcxjGuIohMC.
- [3] P.-S. Laplace, *Recherches sur le calcul intégral et sur le système du monde*, Mém. Acad. Sci. Paris, année 1772, seconde partie (1776), 267–376.
- [4] P. L. Chebyshev, *Mémoire sur les nombres premiers*, J. Math. Pures Appl. **17** (1852), 366–390.
- [5] T. Tao, *An experimental AI-math challenge: using tenth discriminant bounds to explore arguments ruling out Siegel zeroes*, What's new, 20 October 2026. <https://terrytao.wordpress.com/2026/10/20/an-experimental-ai-math-challenge-using-tenth-discriminant-bounds-to-explore-arguments-ruling-out-siegel-zeroes/>.
- [6] R. van Dijk, *A Frobenius determinant proof of the non-existence of Landau–Siegel zeros*, hexagon:2610.00409v2 (2026). <https://hexagonmath.org/2610.00409v2>.