ONE CM DETERMINANT: MERTENS MODULO 4

Prerequisites. Legendre's formula $v_p(r!) = \sum_{e\ge1}\lfloor r/p^e\rfloor$, Stirling's formula, Chebyshev's bound (Problem 6.1.1 in Chapter 6), and the arithmetic of $\mathbb{Z}[i]$. The invariant differential and complex uniformization of an elliptic curve [Si1, §III.5, Ch. VI], and supersingular reduction [Si1, §V.4]. The Jacobi theta function θ_1 [DLMF, §20.2], Cauchy's inequality and the argument principle. Section 15.6 also uses the prime number theorem for arithmetic progressions [MV, §11.3]. From Chapter 12, *Complex tori, theta functions and periods*: Jacobi's function ϑ (Section 12.2). From Chapter 14, *Complex multiplication and reduction at an inert prime*: the congruence $D^p \equiv \lambda D \pmod p$ for a formal group (Section 14.2) and the supersingular reduction of $y^2 = x^3 - x$ at the primes inert in $\mathbb{Z}[i]$ (Section 14.3). Chapter 16, *The invariant derivation at a supersingular prime*, treats the derivation D^p for the lemniscate.

15.1. Mertens from the factorial

Let $\theta(X) := \sum_{p\le X}\log p$. How much of $\log r!$ comes from each prime? Chebyshev's bound $\theta(2n) - \theta(n) \le n\log 4$ is Problem 6.1.1 of Chapter 6.

Problem 15.1.1. $\theta(X) < 2X\log 4$ for $X \ge 1$.

Problem 15.1.2. For $r \ge 1$, $-\theta(r) \le \log r! - r\sum_{p\le r}\frac{\log p}{p} \le r\sum_p \frac{\log p}{p(p-1)}$.

With Stirling's formula, Problems 15.1.1 and 15.1.2 prove the following [Mer].

Theorem 15.1.1 (Mertens)**.** $\sum_{p\le X}\log p/p = \log X + O(1)$ *for* $X \ge 2$.

How much of $\log r!$ comes from each odd class modulo 4? Let

$$S_a(X) := \sum_{p\le X,\ p\equiv a\ (4)} \frac{\log p}{p}.$$

Theorem 15.1.2. $S_a(X) = \frac12\log X + O(1)$ *for* $a = 1, 3$ *and* $X \ge 2$.

This is classical, and the usual proof rests on $L(1,\chi_{-4}) \ne 0$ [MV, Ch. 4]. Since $S_1 + S_3 = \log X + O(1)$, two upper bounds suffice. We replace the factorial by one determinant for each class and take $r = \lfloor X\rfloor$.

15.2. The Gaussian Vandermonde

Let $z_1, \dots, z_r$ be distinct Gaussian integers with $0 \le \operatorname{Re} z, \operatorname{Im} z < \lceil\sqrt{r}\rceil$, and $V := \prod_{j<k}(z_k - z_j)$.

Problem 15.2.1. $|V|^2$ is a positive integer, and $\log|V|^2 \le \binom{r}{2}\log(2r)$.

Problem 15.2.2. If $p \equiv 1 \pmod 4$, then $v_p(|V|^2) \ge r^2/p - r$.

Date: November 25, 2026.

Summing Problem 15.2.2 with weight $\log p$ over $p \le r$ gives $r^2 S_1(r) \le \log|V|^2 + r\theta(r)$. With Problems 15.1.1 and 15.2.1 this proves the following. The counting of coincident pairs follows [PV, §2].

Theorem 15.2.1. $S_1(X) \le \frac{1}{2}\log X + O(1)$.

Problem 15.2.3. If $p \equiv 3 \pmod 4$, then $v_p(|V|^2) \ge r^2/p^2 - r$.

The weights $\log p/p^2$ have a convergent sum, so Problem 15.2.3 says nothing about S_3. An inert prime has residue field $\mathbb{F}_{p^2}$, and Gaussian integers coincide modulo p only with frequency $1/p^2$. To see an inert prime with frequency $1/p$ we use the curve with complex multiplication by $\mathbb{Z}[i]$, which is supersingular exactly at these primes. Its invariant derivation D satisfies $D^p \equiv 0 \pmod p$, so every block of p derivatives gains a factor p, as every block of p consecutive integers does in $r!$.

15.3. The derivation at an inert prime

Let $E\colon y^2 = x^3 - x$, $A := \mathbb{Z}[x,y]/(y^2 - x^3 + x)$, $\omega := dx/(2y)$, and $P := (0,0)$. The derivation D of A dual to ω is

$$Dx = 2y, \qquad Dy = 3x^2 - 1.$$

The automorphism $[i](x,y) := (-x, iy)$ fixes P and pulls ω back to $i\omega$. Let $d_k := (D^k x)(P)$.

Problem 15.3.1. The d_k are integers, and $d_k = 0$ unless $k \equiv 2 \pmod 4$. Moreover $d_2 = -2$, $d_6 = 144$, $d_{10} = -96768$.

Let $s = 1 + \frac{1}{4}t^4 + \cdots$ be the root of $s^4 = 1 + t^4$ with constant term 1. For odd p it lies in $\mathbb{Z}_{(p)}[[t]]$.

Problem 15.3.2. The point $x = -t^2/s^2$, $y = -t/s^3$ lies on E, t is a parameter at P, and

$$\omega = \frac{dt}{s^3} = \sum_{h\ge 0} (-1)^h b_h\, t^{4h}\, dt, \qquad b_h := \frac{\prod_{j=1}^{h}(4j-1)}{4^h h!}.$$

Thus E is a quotient of the Fermat quartic $s^4 = 1 + t^4$, and its differential is a series in t^4.

Problem 15.3.3. Let p be an odd prime. On A/pA the operator D^p is a derivation, and $D^p = cD$ for a constant $c \in \mathbb{F}_p$.

On the formal group of E this is the congruence $D^p \equiv \lambda D \pmod p$ of Section 14.2, with $\lambda \equiv c$.

Problem 15.3.4. If $p \equiv 3 \pmod 4$, then $c = 0$.

This is the vanishing of the Hasse invariant at a supersingular prime [Si1, Thm. V.4.1(a)].

Problem 15.3.5. If $p \equiv 3 \pmod 4$, then $p^{\lfloor k/p \rfloor}$ divides $(D^k f)(P)$ for all $f \in A$ and $k \ge 0$. For instance $3^2 \mid d_6$ and $7^2 \mid d_{14} = 268240896$.

15.4. The determinant of derivatives

Write $E(\mathbb{C}) = \mathbb{C}/\Lambda$ with $dz = \omega$ [Si1, Ch. VI], and let $w(z)$ be the x-coordinate of $P + z$. Then $w(z) = \wp(z + u_0)$ for a lift $u_0 \notin \Lambda$ of P, $D = d/dz$, $d_k = w^{(k)}(0)$, and

$$(w')^2 = 4(w^3 - w), \qquad w(0) = w'(0) = 0, \qquad w''(0) = -2.$$

For $r \geq 1$, let M be the matrix whose row of index $k \geq 0$ lists the kth derivatives at 0 of

$$\frac{z^j}{j!} \quad (0 \leq j < r), \qquad \frac{z^j}{j!}\, w(z) \quad (0 \leq j < r). \tag{1}$$

The first r columns are the identity followed by zeros.

Problem 15.4.1. The entry of M in row k and column $z^j w/j!$ is $\binom{k}{j} d_{k-j}$ for $k \geq j$, and 0 otherwise.

A relation among the columns, restricted to rows $0, \ldots, 4r$, is a pair of polynomials a, b of degree $< r$, not both zero, with $a + bw = O(z^{4r+1})$.

Problem 15.4.2. Let $Q(a, b) := (a'b - ab')^2 + 4ab(a^2 - b^2)$. Then $Q(a, b) = b^4\big((h')^2 - 4(h^3 - h)\big)$ with $h = -a/b$, when $b \neq 0$. If $a + bw = O(z^{4r+1})$ with $\deg a, \deg b < r$, then $Q(a, b) = 0$.

Problem 15.4.3. No nonconstant rational function $h \in \mathbb{C}(z)$ satisfies $(h')^2 = 4(h^3 - h)$.

Problem 15.4.4. If $h \in \{0, \pm 1\}$ and $b \neq 0$ has degree $< r$, then $b(w - h)$ vanishes at 0 to order at most $r + 1$.

Problems 15.4.2–15.4.4 prove the following.

Theorem 15.4.1. *The rows of M of index $0, \ldots, 4r$ have rank $2r$.*

In order of increasing k, keep each row of M that is independent of its predecessors, until $2r$ rows are kept. Their indices are $I = \{0, \ldots, r-1, k_1, \ldots, k_r\}$ with $r \leq k_1 < \cdots < k_r \leq 4r$. Expanding along the identity block,

$$N_r := \det M_I = \det\Big[\tbinom{k_i}{j} d_{k_i - j}\Big]_{1 \leq i \leq r,\ 0 \leq j < r}$$

is a nonzero integer. Let $L := \sum_i k_i - \binom{r}{2}$, the total order $\sum_i (k_i - j_i)$ of the derivatives in each term of this determinant.

Problem 15.4.5. For $r = 1, 2, 3$ the new rows are $\{2\}$, $\{2, 3\}$, $\{3, 4, 6\}$, and $N_r = -2,\ 12,\ 2^7 3^4$.

Problem 15.4.6. $r^2 \leq L \leq 4r^2$, and $v_p(N_r) \geq L/p - r$ for $p \equiv 3 \pmod 4$.

15.5. The size of the determinant

The entries d_k grow like $k!$ times a power of the distance from 0 to the nearest pole of w. To bound N_r we first remove the poles.

Problem 15.5.1. Let H be holomorphic near 0 with $H(0) = 1$. Multiplying all the functions (1) by H does not change $\det M_I = N_r$.

Write $\Lambda = \lambda(\mathbb{Z} + \tau\mathbb{Z})$ with $\operatorname{Im}\tau > 0$, and let

$$\theta_\tau(v) := 2\sum_{n\ge 0}(-1)^n e^{\pi i\tau(n+1/2)^2}\sin\big((2n+1)\pi v\big),$$

so that $\theta_\tau(v) = \theta_1(\pi v \mid \tau)$ [DLMF, (20.2.1)]. In terms of Jacobi's function ϑ of Section 12.2, $\theta_\tau(v) = -i\,e^{\pi i\tau/4+\pi iv}\,\vartheta\big(v+\frac{1+\tau}{2}\big)$. It is odd, $\theta_\tau(v+1) = -\theta_\tau(v)$, and $\theta_\tau(v+\tau) = -e^{-\pi i\tau-2\pi iv}\theta_\tau(v)$.

Problem 15.5.2. The zeros of θ_τ are the points of $\mathbb{Z}+\tau\mathbb{Z}$, and they are simple.

Let $H(z) := \theta_\tau\big((z+u_0)/\lambda\big)^2/\theta_\tau(u_0/\lambda)^2$.

Problem 15.5.3. H and Hw are entire, and $|H(z)|, |H(z)w(z)| \le e^{C(1+|z|^2)}$ with C independent of z.

Problem 15.5.4. For every $R > 0$, $|N_r| \le (2r)!\,(4r/R)^L e^{2Cr(1+R^2)}$. Hence $\log|N_r| \le \frac{1}{2}L\log r + O(r^2)$.

Summing Problem 15.4.6 with weight $\log p$ over $p \le r$ gives $LS_3(r) \le \log|N_r| + r\theta(r)$. By Problems 15.1.1 and 15.5.4, and $L \ge r^2$, this proves the following.

Theorem 15.5.1. $S_3(X) \le \frac{1}{2}\log X + O(1)$.

Theorems 15.1.1, 15.2.1 and 15.5.1 prove Theorem 15.1.2. The proof never uses $L(1,\chi_{-4}) \ne 0$.

15.6. The linear term

Both determinants lose $O(r^2)$: the floors $\lfloor k/p\rfloor$ cost $r\theta(r)$, and the bounds for $|V|$ and $|N_r|$ are crude at order r^2. So they give S_a up to $O(1)$ and say nothing of the constant term. For $\chi = \chi_{-4}$ that term involves

$$c_\chi := \frac{L'}{L}(1,\chi) = \gamma + \log\frac{\pi^2}{2\varpi^2} = 0.2456\ldots, \qquad \varpi := 2\int_0^1 \frac{dt}{\sqrt{1-t^4}},$$

where the second expression follows from Kronecker's limit formula and the value of ϖ in terms of $\Gamma(\frac{1}{4})$ (Theorem 12.3.1); it is the case $\mathbb{Q}(i)$ of the formula of Chowla and Selberg [CS]. How close can a determinant come to c_χ?

On the Vandermonde side the floors can be kept exactly. For a prime power q let $w_q(k) := \sum_{e\ge1}\lfloor k/q^e\rfloor$, and let $k!_{\mathbb{Z}[i]} := \prod_{\mathfrak{p}} \mathfrak{p}^{w_{N\mathfrak{p}}(k)}$, the kth factorial of $\mathbb{Z}[i]$ in the sense of Pólya and Bhargava. For any n Gaussian integers the Vandermonde product is divisible by $\prod_{k<n} k!_{\mathbb{Z}[i]}$ [Bh]. Write $|k!_{\mathbb{Z}[i]}|$ for the absolute value of a generator.

Problem 15.6.1. $\log\dfrac{k!}{|k!_{\mathbb{Z}[i]}|} = \frac{1}{2}w_2(k)\log 2 + \sum_{p\equiv 3\ (4)}\log p\sum_{e\text{ odd}}\Big\lfloor\dfrac{k}{p^e}\Big\rfloor$. For $k = 6$ both sides are $\log 36$.

Let $\beta(n) := \sum_{k<n}\log|k!_{\mathbb{Z}[i]}|$.

Problem 15.6.2. $\beta(n) = \frac{1}{2}\sum_{N<n}(n-N)\big(\log N + \sum_{p^e\mid N}\chi(p^e)\log p\big)$, the inner sum over prime powers $p^e > 1$.

The prime number theorem for χ [MV, §11.3] gives $\sum_{p^e\le x}\chi(p^e)\log p = o(x)$ and $\sum_{p^e\le x}\chi(p^e)\log p/p^e = -c_\chi + o(1)$.

Problem 15.6.3. $\beta(n) = \frac{n^2}{4}\log n - \frac{n^2}{4}\left(\frac{3}{2} + c_\chi\right) + o(n^2)$.

We take the points in a disc.

Problem 15.6.4. Let μ be the uniform probability measure on the disc $|z| \le R$. For $|z| \le R$, $\int \log|z-u|\, d\mu(u) = \log R - (R^2 - |z|^2)/(2R^2)$, and hence $\iint \log|z-u|\, d\mu\, d\mu = \log R - \frac{1}{4}$.

Problem 15.6.5. Let V_n be the Vandermonde product of the n Gaussian integers nearest 0. Then $\log|V_n| = \frac{n^2}{4}\log\frac{n}{\pi} - \frac{n^2}{8} + o(n^2)$.

Problem 15.6.6. $\beta(n) \le \log|V_n|$ implies $c_\chi \ge \log\pi - 1 = 0.1447\ldots$.

So even with exact divisibility the Vandermonde loses $c_\chi - \log\pi + 1 = 0.1008\ldots$ in the linear term. On the side of derivatives one may build Padé-type determinants from the Taylor coefficients of the lemniscatic sine, whose poles are the points of $\varpi\left(\frac{1+i}{2} + \mathbb{Z}[i]\right)$. We expect, from computation, that they give $c_\chi \le \log(4\pi/\varpi^2) = 0.6031\ldots$, short by the absolute constant $\log(8/\pi) - \gamma = 0.3574\ldots$; we do not know a proof of the size estimate this needs. In both directions the loss comes from a disc of Gaussian integers, as nodes on one side and as poles on the other. An error $O(1)$ in S_a is Chebyshev's strength. We expect that one determinant is not enough to control the constant term, let alone the error terms that the Riemann hypothesis requires.

Exercises.

(1) If $p \equiv 1 \pmod 4$ and $h = (p-1)/4$, then $c \equiv (-1)^h b_h \not\equiv 0 \pmod p$ in Problem 15.3.3. This is the coefficient of x^{p-1} in $(x^3 - x)^{(p-1)/2}$: $c = 3, 6, 2$ for $p = 5, 13, 17$.
(2) $N_4 = 2^{12}\,3^5 \cdot 5 \cdot 7$, with new rows $4, 5, 6, 7$.

Hints

§15.1.

15.1.1: Sum Problem 6.1.1 over n near $X/2^m$.
15.1.2: Expand $\log r!$ by Legendre's formula; compare $\lfloor r/p \rfloor$ with r/p, and bound the terms with $e \ge 2$ by a geometric series.

§15.2.

15.2.1: $|V|^2$ is the norm of V.
15.2.2: Let $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, and count the pairs $j < k$ with $z_j \equiv z_k$ modulo $\mathfrak{p}$ and modulo $\bar{\mathfrak{p}}$.
15.2.3: Now $\mathbb{Z}[i]/p \cong \mathbb{F}_{p^2}$, and $p \mid z$ gives $p^2 \mid |z|^2$.

§15.3.

15.3.1: Compute $D^k x$ in A, using $y^2 = x^3 - x$. For the vanishing, compare D with its transform under the automorphism $[i]$, which fixes P.
15.3.2: $4s^3 s' = 4t^3$. Then $dx = -2t\, dt/s^6$. Expand $s^{-3} = (1+t^4)^{-3/4}$ binomially; $y = -t + O(t^5)$.
15.3.3: Leibniz's rule, and $p \mid \binom{p}{i}$ for $0 < i < p$. The derivation D is dual to the regular nowhere vanishing ω, so $D^p = cD$ with c a function regular on all of E.
15.3.4: $c \equiv \lambda \equiv c_p = A_p$ by Problems 14.2.3 and 14.2.6; then Problem 14.3.2.
15.3.5: Lift $D^p A \subseteq pA$ and iterate.

§15.4.

15.4.2: For the second part, substitute $a = -bw + O(z^{4r+1})$, and compare the order of vanishing at 0 with the degree.

15.4.3: The map $z \mapsto (h, h'/2)$ would extend to $\mathbb{P}^1 \to E$ and pull ω back to dz. Look at $z = \infty$.

15.4.4: w has a double zero at 0.

15.4.5: Use Problem 15.4.1 and the values in Problem 15.3.1.

15.4.6: Use $k_i \geq r + i - 1$. Apply Problem 15.3.5 to each term of the determinant, and use $\lfloor m/p \rfloor > m/p - 1$.

§15.5.

15.5.1: Leibniz's rule, and the way the rows I were chosen.

15.5.2: Integrate θ'_τ/θ_τ around a period parallelogram; the sides cancel up to the jump $-2\pi i$ under $v \mapsto v + \tau$. Use oddness for the location.

15.5.3: The double zeros of H sit at the double poles of w. Bound H, Hw on one parallelogram, and translate using the functional equation of θ_τ.

15.5.4: Apply Problem 15.5.1 and Cauchy's inequality to each entry, then choose R.

§15.6.

15.6.1: $2 = -i(1+i)^2$; a split p has two primes of norm p, and an inert p is prime of norm p^2.

15.6.2: By Problem 15.6.1, $\log|k!_{\mathbb{Z}[i]}| = \sum_{p^e} \frac{1+\chi(p^e)}{2} \log p \, \lfloor k/p^e \rfloor$. Then $\sum_{k<n} \lfloor k/d \rfloor = \sum_{N<n,\, d|N} (n - N)$.

15.6.3: $\sum_{1 \leq m < x} (x - m) = \frac{x^2}{2} - \frac{x}{2} + \frac{1}{2}\{x\}(1 - \{x\})$. For the last term with $x = n/d$, treat $d \leq \delta n$ trivially, and use partial summation on each interval where $\lfloor n/d \rfloor$ is constant.

15.6.4: $\frac{1}{2\pi} \int_0^{2\pi} \log|z - \rho e^{i\phi}| \, d\phi = \log \max(|z|, \rho)$.

15.6.5: Scale by $R = \sqrt{n/\pi}$ and compare the sum over pairs with the integral of Problem 15.6.4; compare $\sum \log(|z - u|/R)$ with the integral; pairs at distance $< \varepsilon R$ contribute $O(\varepsilon^2 \log(1/\varepsilon)\, n^2)$.

15.6.6: Compare the coefficients of n^2.

References

[Bh] M. Bhargava, *P-orderings and polynomial functions on arbitrary subsets of Dedekind rings*, J. reine angew. Math. **490** (1997), 101–127.

[CS] A. Selberg and S. Chowla, *On Epstein's zeta-function*, J. reine angew. Math. **227** (1967), 86–110.

[DLMF] *NIST Digital Library of Mathematical Functions*, `https://dlmf.nist.gov/`, Chapter 20.

[Mer] F. Mertens, *Ein Beitrag zur analytischen Zahlentheorie*, J. reine angew. Math. **78** (1874), 46–62.

[MV] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory I. Classical Theory*, Cambridge Stud. Adv. Math. 97, Cambridge University Press, 2007.

[PV] V. V. Volkov and F. V. Petrov, *On the interpolation of integer-valued polynomials*, J. Number Theory **133** (2013), 4224–4232; arXiv:1108.3212.

[Si1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, 2009.