ECC RESEARCH PROGRAM · P2.1

The Auxiliary Curve That Maurer's Reduction Still Lacks

Obstruction theorems, conditional abelian-surface existence, and the two algorithmic gaps in the uniform CDH-to-DLP equivalence

math.st [1] **@math__street** [1]

with GPT 5.6 Sol · Claude Fable 5

[1]Independent research collective, math.st · July 2026

ABSTRACT

Maurer and Wolf reduce the discrete logarithm problem in a cyclic group of prime order r to the computational Diffie–Hellman problem, **given** an auxiliary elliptic curve $E'/\mathbb{F}_r$ whose group order is $(\log r)^{O(1)}$-smooth. The reduction is uniform in everything except that curve: no algorithm is known that constructs it in $\mathrm{poly}(\log r)$ time for every prime r, and this single missing object is what separates a non-uniform equivalence from a uniform one. This paper reports a ten-session research effort on that gap, with partial results on both sides. On the negative side we prove, unconditionally, that every proposed **full** auxiliary group other than an abelian variety fails on an infinite family of primes: the full multiplicative group (via a recent shifted-prime theorem), every full norm-one torus menu of bounded degree, every full algebraic torus of globally bounded dimension, and — via Chevalley decomposition and Lang's theorem — every full connected commutative group with a nonzero affine part. A public-coin counting lemma further eliminates polylog-smooth **selected subgroups** of one-dimensional tori in the recoverable-encoding model. On the positive side, combining a prescribed-order theorem for abelian surfaces with an RH-conditional short-interval smoothness theorem yields: under the Riemann Hypothesis, every sufficiently large prime field admits an ordinary abelian surface with polylog-smooth order, and an explicit genus-two Jacobian of that order would satisfy the Maurer–Wolf interface. Two algorithmic gaps remain and are made exact: finding the smooth order in the central $r^{3/2}$-length interval in polynomial time, and realizing its Weil polynomial as an explicit curve equation. We prove that the audited generic finder routes cannot close the first gap — Boneh's CRT decoder misses the interval for every fixed smoothness exponent above one, and exponent-vector searches either provably miss infinitely many prime centers or inflate into an exponentially precise subset-sum instance. Alongside, seeded experiments through 60 bits quantify blind search, an exact iid-oracle query bound, and the striking finite-size success of bounded-discriminant CM: all 4,096 tested 60-bit primes admit a cubic-log smooth CM order with $|D| \le 60^3$. Every claim carries its epistemic tag; nothing conditional or empirical is promoted to proved.

Keywords. Maurer reduction · CDH · DLP · smooth group orders · CM method · algebraic tori · abelian surfaces

1 Introduction

Let $G = \langle g \rangle$ be cyclic of prime order r. The computational Diffie–Hellman problem (CDH) in G asks for g^{uv} given (g, g^u, g^v); the discrete logarithm problem (DLP) asks for s given g^s. DLP-hardness trivially upper bounds CDH-hardness; the converse — that a CDH oracle suffices to compute discrete logarithms in polynomial time — is the content of the celebrated reduction of Maurer and Wolf [1]. That reduction is not free: it consumes an **auxiliary group**, most naturally an elliptic curve $E'/\mathbb{F}_{r'}$, whose group order must be known and B-smooth for $B = (\log r)^{O(1)}$. Given such a curve, the reduction embeds implicitly represented field elements into implicit curve points and unwinds them with generalized Pohlig–Hellman at cost polynomial in $\log r$ and B. The curve is the whole difficulty. Maurer and Wolf themselves supply it as **side information** and record polylogarithmic smoothness in the Hasse interval as an assumption; twenty-five years later the uniform statement is still open, and practical instantiations [2], [3] remain parameter-by-parameter searches.

Problem P2.1 asks for either resolution: an algorithm that, on input r, constructs in $\mathrm{poly}(\log r)$ time an auxiliary elliptic curve over $\mathbb{F}_{r'}$ (or a related structure) with $(\log r)^{O(1)}$-smooth order — or an infinite family of primes for which no such curve exists or finding one is hard. This paper is the record of a fifteen-sub-goal campaign on that question. Neither branch is closed, and we do not pretend otherwise. What the campaign produced is a set of unconditional obstruction theorems that eliminate every candidate auxiliary family **except** abelian varieties, a conditional existence theorem in dimension two, an exact statement of the two algorithms still missing, and proofs that the standard generic routes to the first of them fail.

Main findings (honest summary). **(i)** PROVED Every full connected commutative auxiliary group of globally bounded dimension with a nonzero affine part — multiplicative groups, all norm-one tori of bounded degree, all algebraic tori of bounded dimension, and their unipotent extensions — admits an infinite family of primes r on which its order has a prime factor $r^{\Omega(1)}$. Only abelian varieties survive. Polylog-smooth selected subgroups of one-dimensional tori are also ruled out in the public-coin recoverable-encoding model.

(ii) CONDITIONAL: Riemann Hypothesis Every sufficiently large prime r admits an **ordinary abelian surface** over $\mathbb{F}_r$ with $(\log r)^{O(1)}$-smooth order, and an explicit genus-two Jacobian with that order would satisfy the full Maurer–Wolf interface. Existence is not construction: a polynomial-time smooth-order finder and an explicit curve-equation seed are both missing, and we prove the audited CRT-decoding and exponent-vector routes cannot supply the finder.

(iii) EMPIRICAL: 4,096 descending 60-bit primes Bounded-discriminant CM covers every tested prime at cubic-logarithmic bounds ($B = |D|_{\max} = 60^3$), yet the same route is asymptotically unsupported under the measured random-integer smoothness model. The uniform small-CM theorem $\mathsf{SCM}_{C,K}$ remains the blocking open question.

1.1 Contributions and scope

We contribute (i) an exact restatement of the Maurer–Wolf requirement and its reduction mechanics in repository notation (§2); (ii) a reproducible blind-search baseline with an exact adaptive lower bound in an explicit oracle model (§3, Figure 1, Figure 2); (iii) the small-CM sufficient condition $\mathsf{SCM}_{C,K}$ with coverage measurements through 60 bits (§4, Figure 3, Figure 4); (iv) the

obstruction theorems for multiplicative groups, tori, affine parts, and selected subgroups (§5); (v) the RH-conditional abelian-surface existence theorem, the genus-two Jacobian interface, and the four-level realization separation (§6); (vi) proofs that Boneh's CRT decoder and the exponent-vector/subset-sum routes miss the required interval scale (§7); and (vii) the precise open frontier (§8).

Everything below is grounded in the research record: theorems are stated with the tags under which they were closed (PROVED , CITED , CONDITIONAL: … , EMPIRICAL: … , HEURISTIC), and finite experiments are never extrapolated beyond their stated ranges (all experiments respect the scaffold ceiling $\log_2 r \le 60$).

2 The Maurer–Wolf reduction and its exact requirement

Throughout, $P^+(N)$ denotes the largest prime factor of a positive integer N, with $P^+(1) = 1$; N is ***B*-smooth** when $P^+(N) \le B$. We write $L = \lceil \log_2 r \rceil$.

2.1 The auxiliary-group interface

A group element g^x is an **implicit representation** of $x \in \mathbb{F}_r$. Implicit addition of representations is multiplication in G, implicit negation is inversion in G, implicit multiplication is one call to the CDH oracle $\mathsf{DH}_g(g^u, g^v) = g^{uv}$, and inversion of a nonzero implicit field element is exponentiation to $r-2$, costing $O(\log r)$ implicit multiplications [1]. The reduction needs an auxiliary finite abelian group H of constant rank that is **strongly algebraically defined** over $\mathbb{F}_r$: group elements have coordinate representations of bounded size, the group operations are given by fixed low-degree algebraic formulas evaluable on implicit inputs, and there are randomized algorithms `EMBED` and `EXTRACT` such that $\texttt{EMBED}(x, e)$ maps a field element into H using public randomness e with bounded expected algebraic cost, and $\texttt{EXTRACT}(\texttt{EMBED}(x, e), e) = x$ [1]. In the prime-order setting relevant here, the group order of G has the single prime divisor r, so the multi-prime hypotheses of the general theorem are vacuous.

> **Proposition 1** (Maurer–Wolf, restated for prime order). CITED Let G be cyclic of prime order r with a CDH oracle, and let H be a constant-rank, strongly algebraically defined abelian group over $\mathbb{F}_r$ with known order N and $P^+(N) \le B$. Then the discrete logarithm in G is computable with $\mathrm{poly}(\log r, B)$ oracle calls and group operations. An elliptic curve $E'/\mathbb{F}_r$ is such a group: it has rank at most two and is strongly $(2, O((\log r)^2))$-algebraically defined [1].

The reduction runs as follows [1], [2]. Given implicit x, choose an explicit uniform shift $e \in \mathbb{F}_r$, set $X = x + e$, and evaluate $D = X^3 + AX + B'$ implicitly on the curve $E' : y^2 = x^3 + Ax + B'$. Test whether D is a quadratic residue (an implicit Legendre-symbol computation) and, when it is — probability $\approx 1/2$ per trial — compute an implicit square root Y. The pair (X, Y) is an implicit point of $E'(\mathbb{F}_r)$. Because $N = \#E'(\mathbb{F}_r)$ is known, B-smooth, and of rank at most two, generalized Pohlig–Hellman over the implicit group makes the point **explicit** using $\mathrm{poly}(\log r, B)$ operations; `EXTRACT` then returns $x = X - e$, and applying this to $x = s$ recovers the input logarithm.

> **Remark 2** (factorization is not an extra hypothesis). PROVED Once N is known and promised B-smooth with $B = (\log r)^C$, trial division through B factors N completely in $\mathrm{poly}(\log r)$ time, so requiring the factorization separately does not strengthen the condition.

The precise object P2.1 asks for is therefore an algorithm producing, for every prime r in time $\mathrm{poly}(\log r)$: a curve equation over $\mathbb{F}_r$ together with the exact value $N = \#E'(\mathbb{F}_r)$ such that $P^+(N) \le (\log r)^C$ for one fixed constant C.

2.2 Existence versus construction

Every elliptic-curve order over $\mathbb{F}_r$ lies in the Hasse interval $[r+1-2\sqrt{r}, r+1+2\sqrt{r}]$, and every integer in that interval occurs as the order of a cyclic curve [1]. Maurer and Wolf define $\nu(r)$ as the least value of P^+ over the interval and obtain their general equivalence **assuming** $\nu(r) = (\log r)^{O(1)}$, with the curve supplied non-uniformly [1]. Two analytic facts bound what current smooth-number technology can say about that assumption. CITED The strongest unconditional all-interval theorem guarantees a y-smooth integer only for $y \ge \exp\big(C(\log x)^{2/3}(\log\log x)^{4/3}\big)$ and interval lengths exceeding $\sqrt{x}$ times a growing factor [4] — both requirements fail the Hasse regime, where y must be polylogarithmic and the length is $4\sqrt{r}$. CITED Under the Riemann Hypothesis, polylogarithmic smoothness in intervals $[x, x+x^\theta]$ is known for every fixed $\theta > 1/2$ [5] — and the Hasse interval sits exactly at the excluded endpoint $\theta = 1/2$. PROVED Consequently neither theorem, nor any checked source, establishes $\nu(r) = (\log r)^{O(1)}$; the existence side is itself open at the Hasse scale, which motivates both the finite experiments of §3–§4 and the dimension-two escape of §6.

3 Blind search: measurements and an exact oracle bound

The naive construction samples curves $y^2 = x^3 + ax + b$ over $\mathbb{F}_r$, counts points, and stops at the first B-smooth order. This section records what that costs at toy scale and what an idealized model proves about it.

3.1 The seeded baseline

EMPIRICAL: one prime per size, 512 curves each, 12–40 bits For the largest prime $r < 2^b$ with $r \equiv 3 \pmod 4$ at each $b \in \{12, 16, \ldots, 40\}$, the script `measure_smooth_orders.py` sampled 512 seeded nonsingular curves, counted each order exactly with a validated BSGS/twist counter (matched against exhaustive enumeration on 36 curves with $101 \le r \le 65519$), and tested smoothness at $B = \lceil L^2 \rceil$ and $B = \lceil L^3 \rceil$. The full run took 20.67 s. Table 1 and Figure 1 give the results against the **exact** B-smooth density of the inclusive Hasse interval, computed by segmented enumeration, with the Dickman approximation shown only as a secondary heuristic.

Table 1: Seeded blind-search success against the exact Hasse-interval baseline (SG-02/SG-03). At 40 bits the quadratic bound first succeeded at candidate 65 and the cubic bound at candidate 6. Data: `measure_smooth_orders_b12-…-40_t512_e2-3_s21012026_20260629_summary.csv`.

bits	succ. /512, $B = L^2$	curve rate	interval rate	succ. /512, $B = L^3$	curve rate	interval rate
12	268	0.5234	0.4275	461	0.9004	0.8118
16	173	0.3379	0.2659	376	0.7344	0.6618
20	103	0.2012	0.1558	292	0.5703	0.5236
24	71	0.1387	0.0902	233	0.4551	0.4090
28	29	0.0566	0.0504	178	0.3477	0.3078
32	21	0.0410	0.0275	121	0.2363	0.2244
36	14	0.0273	0.0147	97	0.1895	0.1630
40	4	0.0078	0.0076	52	0.1016	0.1172

EMPIRICAL: same run Every curve-to-integer rate ratio lay in $[0.867, 1.859]$, so the pre-registered factor-two rejection rule for the random-integer smoothness model did not fire; several small sizes nevertheless fall outside the Wilson interval, so equality of the two distributions was **not** established — the model survives as a working heuristic, no more.

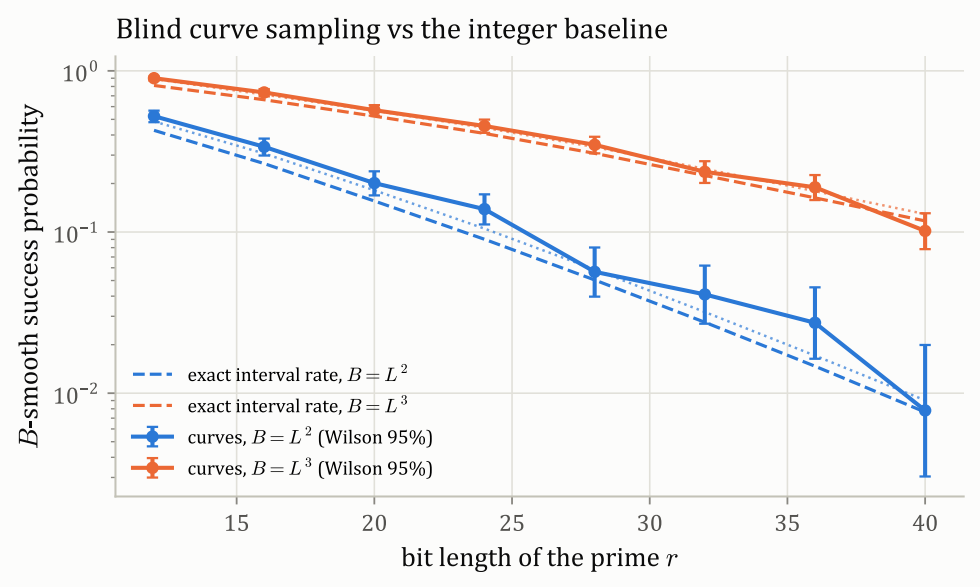

Figure 1: EMPIRICAL: 512 curves/prime, 12–40 bits, seed 21012026 Blind-sampling success probability (markers, Wilson 95% intervals) against the exact interval rate (dashed) and Dickman approximation (dotted) at $B = L^2$ and $B = L^3$. Curve orders track the integer model to within the pre-registered factor-two band throughout.

HEURISTIC Under the very integer model these measurements support, setting $B = (\log r)^C$ gives Dickman parameter $u = \log r/(C \log\log r)$ and expected candidate count $\rho(u)^{-1} = r^{1/C+o(1)}$ — exponential in the input length. Blind search is therefore not the missing algorithm unless curve orders are provably **non**-random in a favorable way; a proved polylogarithmic candidate bound would refute this diagnosis.

3.2 An exact lower bound in the iid Hasse-order oracle

The informal claim "adaptivity cannot help blind sampling" can be made a theorem in an explicit model.

Theorem 3 (optimal adaptive success, iid order oracle). PROVED Fix a prime r, a bound B, the inclusive integer Hasse interval I_r, and its subset S_B of B-smooth values; put $\alpha = |S_B|/|I_r|$. Consider the oracle that assigns every fresh curve label an independent uniform element of I_r (repeat queries return the stored value). Every randomized adaptive algorithm making at most q distinct-label queries succeeds in finding a B-smooth order with probability at most $1 - (1-\alpha)^q$, and q fresh queries attain the bound.

Proof. Fix the algorithm's coins. Conditional on any all-failure transcript, the value at the next fresh label is still independent and uniform on I_r, so it fails with probability exactly $1-\alpha$; induction over the (at most q) fresh queries gives failure probability at least $(1-\alpha)^q$, and repeated labels or early stopping cannot lower it. Averaging over coins proves the randomized bound; querying fresh labels until the first hit attains equality. □

Corollary 4 (least query budgets). PROVED For $0 < \alpha < 1$ and target success $\delta \in (0,1)$, the least admissible budget is $q_\delta = \lceil \log(1-\delta)/\log(1-\alpha) \rceil$.

EMPIRICAL: exact interval counts, 12–40 bits `random_order_lower_bound.py` evaluates the theorem without simulation, using the exact smooth counts of each interval; exhaustive enumeration of all answer sequences at small parameters matched $1-(1-\alpha)^q$ exactly. At 40 bits the idealized 50%/95% budgets are 91/391 queries for $B = L^2$ and 6/25 for $B = L^3$ (Figure 2); A001's observed first hits (65 and 6) are consistent with the idealized medians. This is a consistency check, not evidence of independence — and the theorem is **model-only**: real curve orders are structured, and coefficient-selecting algorithms are outside its scope.

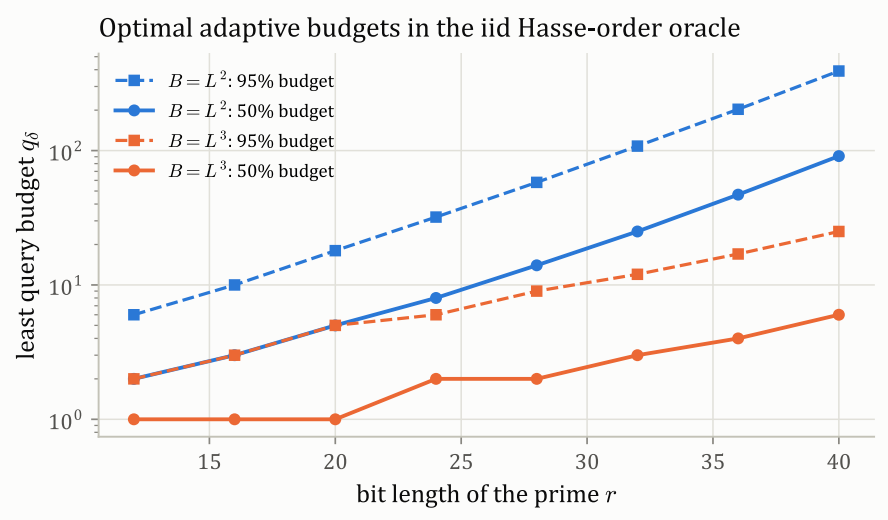

Figure 2: EMPIRICAL: exact Hasse-interval smooth counts, 12–40 bits Exact optimal query budgets $q_{0.50}$ and $q_{0.95}$ in the iid Hasse-order oracle, from `random_order_lower_bound_b12-…-40_e{2,3}_20260629.csv`. The growth tracks α^{-1}, i.e. the reciprocal exact smooth density of the interval.

4 The CM route: a sufficient condition and its finite coverage

Complex multiplication is the one classical technique that constructs a curve **with prescribed order**. Its reach is governed by a single number-theoretic condition that the campaign isolated exactly.

Definition 5 (the small-CM condition $\mathsf{SCM}_{C,K}$). PROVED For fixed constants $C, K > 0$, say $\mathsf{SCM}_{C,K}(r)$ holds when there exist a negative fundamental discriminant D and integers t, v with

$$|D| \le L^K, \quad 4r = t^2 - Dv^2, \quad P^+(r+1-t) \le L^C. \tag{1}$$

The norm equation $4r = t^2 - Dv^2$ is the ordinary-CM reachability criterion [2], and a root of the Hilbert class polynomial H_D modulo r supplies a CM j-invariant [6].

Proposition 6 (witness search is cheap; curve construction is conditional). PROVED If $\mathsf{SCM}_{C,K}(r)$ holds, an integer witness (D, t, v) is findable in randomized expected $\mathrm{poly}(L)$ time: enumerate the $O(L^K)$ fundamental discriminants, solve each norm equation by Cornacchia's algorithm with randomized modular square roots, and trial-divide each candidate order through L^C. CONDITIONAL: certified class-polynomial computation in poly(|D|, log r) time The witness then yields the auxiliary curve: compute and factor H_D modulo r, lift a root to a curve, and select the trace-t twist by exact point counting. Enge's $O(|D| \log^{6+\varepsilon}|D|)$ class-polynomial bound supplies the needed complexity under its explicitly stated floating-point precision heuristic [6]; the rigorous height bound permits certification but the sharp rounding analysis is not itself proved.

Thus a theorem establishing $\mathsf{SCM}_{C,K}(r)$ for **every** prime r would, modulo the stated CM implementation caveat, close P2.1 positively. That theorem is precisely the blocking open question (§8).

4.1 Coverage measurements through 60 bits

EMPIRICAL: 32 primes/size at 12–40 bits; 128 primes/size at 44–60 bits `measure_cm_coverage.py` enumerates the exact $j = 0$ and $j = 1728$ twist-order families (validated exhaustively for $p \in \{7, 13, 17, 19, 31, 37\}$) and all ordinary principal-CM traces with bounded fundamental discriminant (validated against a direct trace scan for $p \in \{101, 211\}$, $|D| \le 200$, and against known class numbers). Figure 3 plots coverage of descending-prime ensembles. At the cubic bounds $B = |D|_{\max} = L^3$, **every** one of the 640 prime/size instances at 44–60 bits succeeded, while the constant-size explicit families decayed from 52/128 (44 bits) to 15/128 (60 bits) — matching the prediction that a constant candidate list must fade.

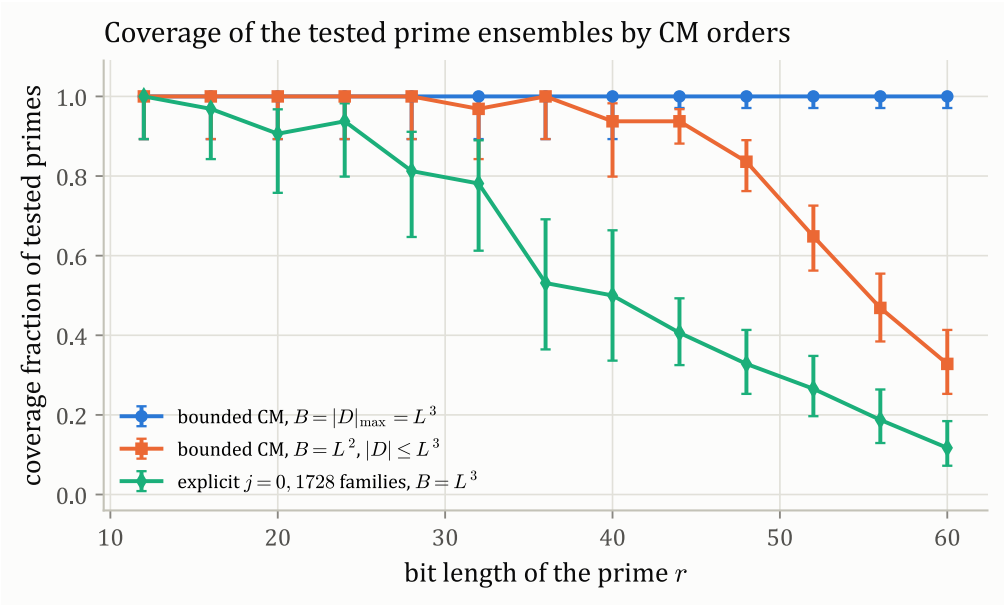

Figure 3: EMPIRICAL: descending-prime ensembles, 12–60 bits Coverage by bounded-discriminant CM and by the explicit $j = 0, 1728$ families, with Wilson 95% intervals. Ensembles: 32 primes per size through 40 bits, 128 per size at 44–60 bits (discriminant bound L^3 throughout). Sources: `measure_cm_coverage_b12-…-40_p32_e2-3_d3` and `…_b44-…-60_p128_e2-3_d3` summary CSVs.

EMPIRICAL: 4,096 descending 60-bit primes The large 60-bit scan sharpens the picture. With $B = 60^3 = 216000$: bounded CM with $|D| \le 60^3$ covered 4096/4096 (Wilson lower endpoint 0.99906); tightening the discriminant to $|D| \le 60^2 = 3600$ dropped coverage to 3635/4096 (rate 0.88745, CI 0.87741–0.89677); the explicit families covered 445/4096 (0.10864). Eight-worker wall times were 42.95 s and 28.50 s. The hardest tested instance by the pre-registered least-discriminant metric was $r = 1152921504606838643 \equiv 11 \pmod{12}$, whose first hit needed $|D| = 180331$ with class number 87, $v = 2899546$, $t = 1759425224$, and order largest prime factor 10,559 — a hardest **tested** case, not a proved worst case.

EMPIRICAL: same 4,096-prime run Coverage at $|D| \le 60^2$ shows a strong residue effect modulo 12 (Figure 4): 97.07% for $r \equiv 1$ but 76.48% for $r \equiv 11$. PROVED The explicit-family half of this ordering has a concrete explanation: the explicit list contains 10, 5, 7, and 1 distinct candidate orders according as $r \bmod 12 = 1, 5, 7, 11$ — the $j = 1728$ family splits when $r \equiv 1 \pmod 4$ and the $j = 0$ family when $r \equiv 1 \pmod 3$.

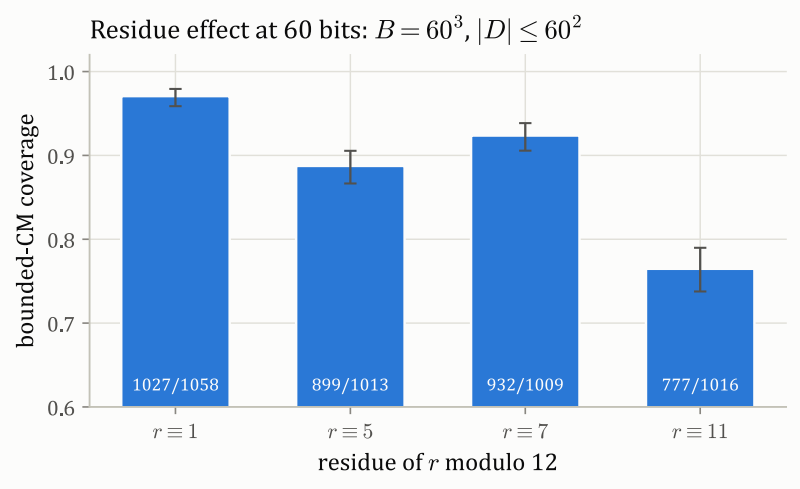

Figure 4: EMPIRICAL: 4,096 descending 60-bit primes, B=60³, |D|≤60² Bounded-CM coverage by residue class of r modulo 12, with Wilson 95% intervals and success counts. Source: `measure_cm_coverage_b60_p4096_e3_d2_w8_20260625_residues.csv`.

4.2 Why finite coverage does not settle the asymptotics

HEURISTIC For fixed C, K, the bounded scan exposes only $O(L^K)$ candidate orders. If their smoothness behaves like that of independent integers near r — the model the §3 measurements support — a union bound gives success probability at most $L^K r^{-1/C+o(1)} \to 0$. At 60 bits the bound $L^3 = 216000 \approx 2^{17.7}$ is far from the regime where this estimate bites, so the perfect finite coverage and the pessimistic asymptotic assessment are **consistent**. A proved correlation between small CM discriminants and smooth norm-equation orders would falsify the assessment; so would a proved anti-correlation falsify the route. Neither exists. This tension — finite usefulness versus worst-case ignorance — is the honest summary of the CM branch.

5 Obstruction theorems: everything full except abelian varieties fails

Maurer–Wolf allow any constant-rank strongly algebraically defined abelian auxiliary group, not only curves [1]. This section closes, one class at a time, every such candidate whose **full** rational-point group is used, leaving only abelian varieties standing. All results in this section are unconditional.

5.1 Full multiplicative groups

If $P^+(r-1) \le (\log r)^C$, the group $\mathbb{F}_r^\times$ itself is a valid auxiliary — the den Boer route, made concretely efficient in [7] — and no curve is needed. But this cannot be uniform:

> **Proposition 7** (the full $\mathbb{F}_r^\times$ route fails on infinitely many primes). PROVED For every fixed C there are infinitely many primes r with $P^+(r-1) > (\log r)^C$; consequently the full multiplicative group, and the full extension groups $\mathbb{F}_{r^n}^\times$ for every $n \ge 1$, are not uniform auxiliary groups.

Proof. CITED Li's shifted-prime theorem gives infinitely many primes with $P^+(r-1) > r^{0.679}$ [8], and $r^{0.679}$ eventually exceeds every fixed power of $\log r$. Since $r - 1 \mid r^n - 1$, the same family obstructs every full extension group; the additive group is unusable outright since its order is r. □

5.2 One-dimensional tori and bounded norm-one menus

The natural repair is the quadratic norm-one torus: for a nonsquare $d \in \mathbb{F}_r$,

$$T_d(\mathbb{F}_r) = \{(x, y) : x^2 - dy^2 = 1\}, \quad (x, y)(u, v) = (xu + dyv, xv + yu), \tag{2}$$

the kernel of the norm $\mathbb{F}_{r^2}^\times \to \mathbb{F}_r^\times$, cyclic of order $r + 1$. PROVED The rational maps

$$t \mapsto \left(\frac{1 + dt^2}{1 - dt^2}, \frac{2t}{1 - dt^2}\right), \qquad t = \frac{y}{x + 1} \tag{3}$$

are mutually inverse between $\mathbb{F}_r$ and $T_d(\mathbb{F}_r) \setminus \{(-1, 0)\}$ (the denominator cannot vanish since d is a nonsquare), so the torus is a strongly algebraically defined auxiliary of rank one whenever $r + 1$ is smooth. EMPIRICAL: exhaustive, (r,d) = (7,3),(11,2),(13,2),(17,3) The parametrization, extraction, point count $r + 1$, and group-law closure were verified exhaustively at toy scale (`torus_alternative.py`). The menu $\{r - 1, r + 1\}$, however, is also not uniform:

> **Theorem 8** (simultaneous obstruction for $r - 1$ and $r + 1$). PROVED There are an absolute constant $c > 0$ and infinitely many primes r with
>
> $$\min\{P^+(r - 1), P^+(r + 1)\} \geq c\, r^{1/10.4}. \tag{4}$$
>
> Hence for every fixed C', no algorithm choosing between the two full one-dimensional tori meets $(\log r)^{C'}$-smoothness for every prime.

Proof. For large X pick primes $q \in (X, 2X)$ and $s \in (2X, 4X)$ and choose by CRT a residue a with $a \equiv 1 \pmod q$ and $a \equiv -1 \pmod s$. Linnik's theorem with Xylouris's admissible exponent $L_0 = 5.2$ [9] supplies a prime $r \equiv a \pmod{qs}$ with $r \leq C(qs)^{L_0} = O(X^{2L_0})$. Then $q \mid r - 1$ and $s \mid r + 1$, so both largest prime factors are at least $X \geq c\, r^{1/(2L_0)}$, and letting $X \to \infty$ yields an infinite family. □

PROVED The same CRT–Linnik synthesis extends to every **fixed finite degree menu**: choosing for each $2 \leq n \leq D$ a comparable prime $q_n \equiv 1 \pmod n$ (fixed-progression PNT [10]) and a residue of exact order n modulo q_n forces $q_n \mid (r^n - 1)/(r - 1)$ for one Linnik prime r simultaneously for all $n \leq D$, with $q_n \geq c_D r^{1/(DL_0)}$. Thus every globally bounded-degree menu of full norm-one tori is obstructed on an infinite prime family.

PROVED On the constructed family the standard random-shift subgroup repair also fails: a $(\log r)^{C'}$-smooth subgroup must omit the forced prime factor, so its size is $O(r^{1-\eta})$ with $\eta = 1/(2L_0)$, and a uniform shift lands in it with probability $O(r^{-\eta})$ per attempt. This bound is for the explicit shift-and-test model only.

5.3 All full algebraic tori of bounded dimension

> **Theorem 9** (torus obstruction, general form). PROVED For every fixed $D \geq 1$ there are constants $c_D, \eta_D > 0$ and infinitely many primes r such that **every** nontrivial full algebraic torus $T/\mathbb{F}_r$ of dimension at most D satisfies $P^+(|T(\mathbb{F}_r)|) \geq c_D\, r^{\eta_D}$ — even when the torus is chosen after seeing r.

Proof. CITED A d-dimensional torus has $|T(\mathbb{F}_r)| = \det(rI - \Phi)$ for the finite-order integral Frobenius action Φ on its rank-d character lattice [11]. Since Φ has finite order, its characteristic polynomial factors as $\prod_n \Phi_n(x)^{e_n}$ into cyclotomic polynomials with $\sum_n e_n \varphi(n) = d$, so

$|T(\mathbb{F}_r)| = \prod_n \Phi_n(r)^{e_n}$. Only indices in $\mathcal{N}_D = \{n : \varphi(n) \le D\}$ can occur, and $\mathcal{N}_D$ is finite: if $p^a \mid n$ then $p^{a-1}(p-1) \mid \varphi(n)$. Put $k_D = |\mathcal{N}_D|$. For large X choose distinct primes $\ell_n \in (X, 2X)$ with $\ell_n \equiv 1 \pmod n$ for each $n \in \mathcal{N}_D$ [10], residues b_n of exact multiplicative order n modulo ℓ_n (with $b_1 = 1$), and combine by CRT; Linnik [9] gives a prime r congruent to that residue with $r = O\big(X^{k_D L_0}\big)$. Taking $X > D + 1$, the exact-order criterion forces $\ell_n \mid \Phi_n(r)$ for every $n \in \mathcal{N}_D$, so every possible cyclotomic factor of every admissible torus order simultaneously contains a prime $\ge X \ge c_D r^{1/(k_D L_0)}$. Set $\eta_D = 1/(k_D L_0)$. □

5.4 Affine parts reduce everything to abelian varieties

Theorem 10 (Chevalley reduction). PROVED Among full rational-point groups of smooth connected commutative algebraic groups of globally bounded dimension over $\mathbb{F}_r$, every candidate with a nonzero affine part is obstructed on an infinite prime family. The only surviving full connected class is that of abelian varieties.

Proof. Chevalley's theorem gives a unique exact sequence $1 \to L \to G \to A \to 1$ with L smooth connected affine commutative and A an abelian variety [12]. Over the perfect field $\mathbb{F}_r$ the unipotent radical $U \subseteq L$ is split with $|U(\mathbb{F}_r)| = r^{\dim U}$, and $T = L/U$ is a torus [13]. Lang's theorem [14] makes the rational-point maps to connected quotients surjective, so the orders multiply: $|G(\mathbb{F}_r)| = |U(\mathbb{F}_r)| \cdot |T(\mathbb{F}_r)| \cdot |A(\mathbb{F}_r)|$. If $\dim U > 0$, the order is divisible by r itself and is never polylog-smooth. If U is trivial and T nontrivial, the torus theorem above supplies the infinite family, and $|T(\mathbb{F}_r)|$ divides the full order. What remains is L trivial, i.e. $G = A$. □

5.5 Selected subgroups in dimension one

Full-group obstructions leave open the idea of embedding into a **smooth subgroup** that omits the forced factor. A counting argument closes this in dimension one, in the model that matters for the reduction.

Lemma 11 (public-coin counting). PROVED Let S be a finite input set, H a finite target group, and let public randomness e (independent of $x \in S$) select an encoder $f_e : S \to H \cup \{\perp\}$ such that a decoder d satisfies $d(e, f_e(x)) = x$ whenever $f_e(x) \ne \perp$. Then

$$\frac{1}{|S|} \sum_{x \in S} \Pr_e[f_e(x) \ne \perp] \le \frac{|H|}{|S|}. \tag{5}$$

Proof. For fixed e, the successful restriction of f_e is injective — two successful inputs sharing an image would force the decoder to return two values on one pair (e, h). Hence the number of successful inputs at each e is at most $|H|$; average over e. □

Corollary 12 (no smooth selected subgroup of a one-dimensional torus). PROVED On the prime family of the torus obstruction, any $(\log r)^C$-smooth subgroup H of a one-dimensional torus omits a prime factor $\ell \ge c r^\eta$ of the ambient order $O(r)$, so $|H| = O(r^{1-\eta})$; with $S = \mathbb{F}_r$, every correct public-coin recoverable encoding into H has average success $O(r^{-\eta})$. No such encoding has inverse-polylogarithmic success on every input.

PROVED The same count does **not** close dimension two or higher: an ambient order near r^d can lose a factor r^η and still contain r elements. Higher-dimensional selected subgroups, private-coin encodings, and abelian varieties are exactly the branches the lemma leaves open — which is where the next section goes.

6 The abelian-surface branch: conditional existence, explicit interface, missing seed

Dimension two enlarges the order interval from Hasse's $4\sqrt{r}$ to $\Theta(r^{3/2})$ around r^2, moving the smooth-number problem off the excluded endpoint $\theta = 1/2$. This buys a conditional theorem — and isolates precisely what a construction still lacks.

6.1 Conditional existence

Theorem 13 (polylog-smooth surface orders exist under RH). CONDITIONAL: Riemann Hypothesis For every sufficiently large prime r there is an integer N with $P^+(N) \le (\log r)^{O(1)}$ in the central interval $\left[r^2 - \lambda r^{3/2}, r^2 + \lambda r^{3/2}\right]$ (any fixed $1/2 < \lambda < 4 - 2\sqrt{2}$), and N is the order of an ordinary abelian surface over $\mathbb{F}_r$.

Proof. (Sketch; the full synthesis is recorded in attempt A007.) CITED For any fixed $0 < \lambda < 4 - 2\sqrt{2}$ and all large r, **every** integer in the displayed interval is the order of an ordinary abelian surface over $\mathbb{F}_r$ — the fixed-dimension prescribed-order theorem [15] (Theorem 1.7, Remark 1.11). The interval has length $\Theta(r^{3/2}) = \Theta(X^{3/4})$ around $X = r^2$, so it contains a subinterval $\left[X, X + X^{3/4}\right]$. CITED Under RH, the short-interval smoothness theorem of [5] (Theorem 1.3) at $\theta = 3/4$ counts y-smooth integers there asymptotically for $y = (\log X)^{K(3/4)}$; positivity of the count supplies the required N, and $\log X = (2 + o(1)) \log r$ makes y polylogarithmic in r. PROVED The synthesis is unavailable unconditionally from the checked sources: Younis's unconditional range at $\theta = 3/4$ requires $y \ge \exp\left((\log X)^{2/3+\varepsilon}\right)$, which is super-polylogarithmic. □

6.2 An explicit genus-two Jacobian would suffice

Proposition 14 (the Jacobian interface). PROVED Let $C : y^2 = f(x)$ be an explicitly supplied nonsingular genus-two curve over $\mathbb{F}_r$ (f squarefree of degree five) with known $(\log r)^{O(1)}$-smooth Jacobian order. Then $J(C)(\mathbb{F}_r)$ is a constant-rank strongly algebraically defined Maurer–Wolf auxiliary group.

Proof. Jacobian elements have constant-size Mumford representations and Cantor's algorithm performs the group law in a constant number of bounded-degree polynomial operations [16], so the group is strongly algebraically defined. For embedding: given implicit x and public random e, set $X = x + e$, test whether $f(X)$ is a square, and on success take an implicit square root Y; the divisor class $[(X, Y) - \infty]$ has Mumford representation $u(z) = z - X$, $v(z) = Y$, and extraction reads X from u and returns $X - e$. The Weil bound $\left|\sum_{X \in \mathbb{F}_r} \chi(f(X))\right| \le 4\sqrt{r}$ makes each trial succeed with probability $1/2 + O(r^{-1/2})$, so the expected number of trials is bounded. Finally, for every prime $\ell \ne r$ the ℓ-torsion of a two-dimensional abelian variety embeds in $(\mathbb{Z}/\ell\mathbb{Z})^4$, so the group rank is at most four — a constant. □

6.3 Four output levels, and where the seed problem sits

PROVED The following outputs are logically distinct, and only the last is a Maurer–Wolf auxiliary: (1) an integral degree-four Weil polynomial f with $f(1) = N$; (2) a Honda–Tate certificate that an isogeny class with polynomial f exists [15]; (3) a Howe–Nart–Ritzenthaler certificate that the class contains a genus-two Jacobian [17]; (4) an explicit curve equation with group law and recoverable `EMBED`/`EXTRACT`. Levels 1–3 specify coefficients, an isogeny class, and an existence predicate — no projective model and no coordinate algorithms.

EMPIRICAL: r = 251, 1019, 4091, 16363 The exact ordinary cases of the HNR criterion are implementable with integer arithmetic alone; `surface_jacobian_scan.py` enumerated every degree-four ordinary Weil polynomial over four toy fields and intersected the resulting order sets with segmented smoothness masks (Table 2). Every integer in all four central intervals — 4.78 million integers in total, including every $\lfloor L^3 \rfloor$-smooth one — was the order of a Jacobian-containing isogeny class. This strengthens the finite existence picture and constructs **no** curve: the criterion certifies, it does not realize.

Table 2: Exhaustive HNR scan of the central intervals $\left[r^2 - \lfloor r^{3/2} \rfloor, r^2 + \lfloor r^{3/2} \rfloor\right]$ (SG-14). Every interval integer, smooth or not, had an ordinary Jacobian-admissible Weil polynomial. Runtimes: 1.39 s (first three fields), 10.58 s (14-bit field). Data: `surface_jacobian_scan_b8-10-12_e3` and `_b14_e3` CSVs.

r	interval integers	ordinary orders	Jacobian-admissible	L^3-smooth	smooth admissible
251	7,953	7,953	7,953	3,038	3,038
1,019	65,057	65,057	65,057	17,379	17,379
4,091	523,329	523,329	523,329	97,059	97,059
16,363	4,186,243	4,186,243	4,186,243	528,541	528,541

PROVED The realization gap is a **seed problem**. Genus-two CM constructions with prescribed Jacobian order have exponential worst-case complexity [18], and the heuristic polynomial-time algorithm in the same work prescribes $\#C(\mathbb{F}_p)$ — the curve's point count, not its Jacobian order — so it solves a different inverse problem. An isogeny walk cannot start without an explicit member of the target class, since isogenous varieties share the Frobenius polynomial and walking presupposes a model to walk from. And an abstract finite group of order N, even with ideal-module data, instantiates neither the algebraic `EMBED` map from implicit field elements nor extraction — the interface a Jacobian gets from its Mumford coordinate ($u(z) = z - (x + e)$ is **readable**), which an arbitrary explicit surface would still have to supply separately.

Two exact algorithmic gaps therefore remain in this branch:

The two missing algorithms (surface branch). **(F)** PROVED Given r, find a $(\log r)^{O(1)}$-smooth integer in the central $r^{3/2}$-length interval around r^2 in $\mathrm{poly}(\log r)$ time. (Existence is guaranteed under RH; the analytic proof enumerates nothing.)

(R) PROVED Given (r, N), output an explicit strongly algebraically defined abelian surface of order N — an explicit genus-two Jacobian suffices — in $\mathrm{poly}(\log r)$ time. (Honda–Tate and HNR certify existence at every tested scale; no checked route outputs an equation.)

7 Why the audited smooth-order finders fail

Gap (F) looks approachable: the target interval is long ($X^{3/4}$ at scale $X = r^2$) and, under RH, provably contains smooth integers. The campaign audited the standard algorithmic routes and closed each with a proof. Throughout, $L = \log X$ and the smoothness threshold is $y = L^K$ for fixed $K > 1$.

7.1 Boneh's CRT decoder misses the interval

CITED Boneh's method finds every integer N in an interval $I = [U, V]$, $H = V - U$, whose gcd with $S = \prod_{p<s} p^{\lfloor \log_p s \rfloor}$ exceeds a threshold $T > S^{\varepsilon}$, where $\varepsilon = \sqrt{\log(4H)/\log S} + 5/(4d)$ for a degree parameter d; if $V < 2T$, every **strongly s-smooth** integer (all prime powers at most s) in I is found [19].

Proposition 15 (radius mismatch at polylogarithmic smoothness). PROVED At the surface scales $U \asymp X$, $H = X^{3/4+o(1)}$, listing all strongly smooth values forces $\log T = (1 + o(1))L$, and a necessary limit of Boneh's sufficient condition is $\log(4H) < (\log T)^2/\log S$. With $s = L^K$, the prime number theorem gives $\log S = (1 + o(1))s = L^{K+o(1)}$, so the right side is $L^{2-K+o(1)} = o(L)$ while $\log H = (3/4 + o(1))L$. The decoder inequality fails for every choice of d — even when the target is promised strongly s-smooth.

PROVED The only asymptotic window the decoder does reach is $s = c \log X$ with $1 \le c \le 4/3$: reaching a divisor of S near X needs $c \ge 1$, and width $X^{3/4}$ needs $c \le 4/3$. But strongly $c \log X$-smooth integers are globally sparse — every one divides S and $\log \tau(S) \le \pi(s) \log(1 + \log s/\log 2) = o(\log X)$, so there are at most $X^{o(1)}$ of them in total, and at most a fraction $X^{-1/4+o(1)}$ of the disjoint length-$X^{3/4}$ intervals in $[X, 2X]$ contains one. No checked existence theorem places one in the special intervals centered at r^2; Younis's theorem counts **ordinary** smooth integers, a much larger class.

7.2 Bounded-support products miss infinitely many prime centers

The next route represents the target as $N = \prod_{p \le y} p^{e_p}$ and searches exponent vectors.

Theorem 16 (bounded-support coverage obstruction). PROVED Fix constants $K, k, C > 0$ and let $y = L^K$. In every sufficiently large dyadic range, some prime $r \in \left[\sqrt{X}, \sqrt{2X}\right]$ has **no** y-smooth integer supported on at most k distinct primes within distance $Cr^{3/2}$ of r^2 — even when the k supporting primes may be chosen from the whole factor base after seeing r.

Proof. Each admissible product in $[X/2, 3X]$ has every exponent $O(L)$ and its support inside a set of $\pi(y) = O(L^K)$ primes, so the number of such products is at most $\sum_{j=0}^{k} \binom{\pi(y)}{j} O(L)^j = L^{O_{K,k}(1)}$, polynomial in L. For one fixed $N \asymp X$, the condition $|N - r^2| \le Cr^{3/2}$ confines r to an interval of length $O_C(X^{1/4})$, since $\left|r - \sqrt{N}\right| = |r^2 - N|/\left(r + \sqrt{N}\right)$ with $r, \sqrt{N} \asymp \sqrt{X}$. All bounded-support products together therefore cover at most $X^{1/4} L^{O_{K,k}(1)}$ prime centers, while the prime number theorem puts $\Theta\left(\sqrt{X}/L\right)$ primes in $\left[\sqrt{X}, \sqrt{2X}\right]$. Since $X^{1/4} L^{O(1)} = o\left(\sqrt{X}/L\right)$, some prime center is missed. □

7.3 Growing support hits an exponential-precision barrier

Proposition 17 (the safe rounding is exponentially precise). PROVED Encode an unrestricted exponent vector as a 0–1 subset sum by giving each prime $p \le y$ up to $\lfloor \log(3X)/\log p \rfloor$ copies of the weight $\log p$; the item count m satisfies $L^{K+o(1)} \le m \le L^{K+1+o(1)}$. The target logarithmic interval has width $\Delta = \log(1 + H/X) = \Theta\left(X^{-1/4}\right)$, so a worst-case safe rounding at scale Q needs $m/Q = O(\Delta)$, i.e. $Q = \Omega\left(mX^{1/4}\right)$, and the rounded integer target has size $t = \Theta(QL) = X^{1/4} L^{O_K(1)}$ — exponential in the input length.

CITED Substituting this target into Bringmann's $\tilde{O}(n + t)$ subset-sum algorithm [20] gives exponential time in L: the algorithm is pseudopolynomial, near-linear in the **numerical** target.

PROVED The lattice alternative fares no better: at the minimal safe scale the rounded instance has $\log_2(\max_i a_i) = \Theta(L)$ and density $m/\log_2(\max_i a_i) \to \infty$ for every fixed $K > 1$, far outside the low-density regime of the Lagarias–Odlyzko success theorem [21] — which is in any case distributional ("almost all instances"), whereas repeated rounded copies of $\log p$ form a highly structured instance. CITED The practical Smooth Subsum Search heuristic is explicitly presented as a factorization heuristic and supplies no every-interval worst-case theorem [22].

PROVED Scope of these negatives: they close the audited generic routes — bounded-support enumeration, pseudopolynomial dynamic programming on the standard rounding, and low-density lattice guarantees. They are **not** an impossibility theorem for every algorithm; a specialized method exploiting the Diophantine structure of prime logarithms, or a different representation of smooth values, is not covered. Under a polynomial-time oracle for the structured logarithmic interval-subset-sum instance, the finder gap (F) would close and only the realization gap (R) would remain.

8 What remains open

The blocking question, recorded as P2.1/Q005, now has an exact shape.

The uniform small-CM theorem. Prove that for some fixed C, K, every prime r satisfies $\mathsf{SCM}_{C,K}(r)$ — i.e. the norm-equation family $\{r + 1 - t : 4r = t^2 - Dv^2, |D| \le L^K\}$ of $O(L^K)$ candidate orders always contains an L^C-smooth member. The 4,096-prime experiment makes this plausible at 60 bits and the random-integer heuristic makes it implausible asymptotically; a proved correlation in either direction would be decisive. Together with a certified CM implementation [6], a positive answer closes P2.1.

The two surface algorithms. Under RH the existence side is settled in dimension two; gaps (F) and (R) of §6 are precisely what remain. For (F), §7 shows the answer must exploit structure the generic routes ignore. For (R), the missing step is a single explicit genus-two Jacobian seed in a prescribed isogeny class — CM is exponential [18], walks need a seed, and abstract groups lack the embedding interface.

Higher-dimensional selected subgroups. The public-coin counting lemma dies in dimension two ($|H| \ge r$ survives the forced-factor loss). The recorded next action is an audit of higher-dimensional selected subgroups and cofactor-projection encodings, where the dimension-one cardinality obstruction no longer applies.

The hardness branch. P2.1′s alternative resolution — an infinite prime family on which no polylog-smooth auxiliary curve exists, or finding one is hard — is equally open. The obstruction technology of §5 (CRT + Linnik against explicit order polynomials) does not apply to curve orders, whose traces do not factor through cyclotomic values; and the iid-oracle bound of §3 is model-only. No lower bound is known in a model containing the real algebraic construction algorithms.

9 Conclusion

P2.1 asked for a uniform polynomial-time construction of a polylog-smooth auxiliary curve — the one missing ingredient of the Maurer CDH-to-DLP equivalence — or evidence that none exists. Ten sessions produced a partial but sharply structured answer. Unconditionally: every full connected commutative auxiliary group with any affine part is dead on an infinite prime family,

by a single CRT–Linnik mechanism pushed through the character lattice and Chevalley decomposition (§5); dimension-one selected subgroups are dead in the recoverable-encoding model; and the generic smooth-order finders — CRT decoding, bounded-support products, safe-rounded subset sums — are dead at the surface interval scale (§7). Conditionally: under RH, a polylog-smooth ordinary abelian-surface order exists over every large prime field, and an explicit genus-two Jacobian of that order would finish the reduction (§6). Empirically: bounded-discriminant CM covers every tested prime through 60 bits at cubic bounds, while its asymptotic status hangs on an unproved correlation (§4). The frontier is exact: prove $\mathsf{SCM}_{C,K}$ uniformly, or find the smooth surface order and its Jacobian seed in polynomial time, or push the obstructions into abelian varieties themselves. None of these is closed here, and we have been careful to claim only what the record supports.

Reproducibility

All experiments run under Python 3.13 on the repository's deterministic harness; every executable module carries known-answer tests (315 repository tests pass, including six P2.1 validation entry points). The measurement scripts are `measure_smooth_orders.py` (seeded blind search; BSGS/twist counter validated against exhaustive enumeration; 20.67 s full run), `measure_cm_coverage.py` (norm-equation and explicit-family scan; Cornacchia solving, class numbers via reduced forms, Wilson intervals; 747.32 s serial five-size run, 28.50 s and 42.95 s for the eight-worker 4,096-prime runs), `summarize_cm_residues.py` (residue aggregation), `random_order_lower_bound.py` (exact iid-oracle budgets, no Monte Carlo), `torus_alternative.py` (exhaustive norm-one torus validation), and `surface_jacobian_scan.py` (exact ordinary HNR criterion; 1.39 s and 10.58 s recorded runs). The figures in this paper are generated directly from the recorded CSVs: `measure_smooth_orders_…_summary.csv` (Figure 1), `random_order_lower_bound_…_e{2,3}.csv` (Figure 2), `measure_cm_coverage_…_{p32,p128}_…_summary.csv` (Figure 3), and `measure_cm_coverage_b60_p4096_e3_d2_w8_…_residues.csv` (Figure 4). Every mathematical claim above carries the epistemic tag under which it was closed in the research log; untagged sentences are exposition, not claims. Finite ensembles are deterministic toy experiments through $\log_2 r \leq 60$ and are never universal proof.

References

[1] U. M. Maurer and S. Wolf, "The relationship between breaking the Diffie–Hellman protocol and computing discrete logarithms," *SIAM Journal on Computing*, vol. 28, no. 5, pp. 1689–1721, 1999, doi: 10.1137/S0097539796302749.

[2] A. Muzereau, N. P. Smart, and F. Vercauteren, "The equivalence between the DHP and DLP for elliptic curves used in practical applications," *LMS Journal of Computation and Mathematics*, vol. 7, pp. 50–72, 2004, doi: 10.1112/S1461157000001042.

[3] A. May and C. R. T. Schneider, "Dlog is practically as hard (or easy) as DH – solving dlogs via DH oracles on EC standards," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2023, no. 4, pp. 146–166, 2023, doi: 10.46586/tches.v2023.i4.146-166.

[4] S. Jain, "Existence of smooth numbers in short intervals," *The Quarterly Journal of Mathematics*, vol. 77, no. 2, pp. 397–422, 2026, doi: 10.1093/qmath/haag010.

[5] K. Younis, "Asymptotics for smooth numbers in short intervals." 2024.

[6] A. Enge, "The complexity of class polynomial computation via floating point approximations," *Mathematics of Computation*, vol. 78, no. 266, pp. 1089–1107, 2009.

[7] M. F. Bollauf, R. Parisella, and J. Siim, "Revisiting discrete logarithm reductions," *IACR Communications in Cryptology*, vol. 2, no. 2, 2025, doi: 10.62056/a0c3c3c2h.

[8] R. Li, "An average Brun–Titchmarsh theorem and shifted primes with a large prime factor." 2025.

[9] T. Xylouris, "Über die Linniksche Konstante." 2009.

[10] I. Soprounov, "A short proof of the prime number theorem for arithmetic progressions." 1998.

[11] V. V. Batyrev and Y. Tschinkel, "Rational points of bounded height on compactifications of anisotropic tori," *International Mathematics Research Notices*, vol. 1995, no. 12, pp. 591–635, 1995, doi: 10.1155/S1073792895000365.

[12] B. Conrad, "A modern proof of Chevalley's theorem on algebraic groups," *Journal of the Ramanujan Mathematical Society*, vol. 17, no. 1, pp. 1–18, 2002.

[13] B. Conrad, "Finiteness theorems for algebraic groups over function fields," *Compositio Mathematica*, vol. 148, no. 2, pp. 555–639, 2012.

[14] S. Lang, "Algebraic groups over finite fields," *American Journal of Mathematics*, vol. 78, no. 3, pp. 555–563, 1956, doi: 10.2307/2372673.

[15] R. van Bommel, E. Costa, W. Li, B. Poonen, and A. Smith, "Abelian varieties of prescribed order over finite fields," *Mathematische Annalen*, vol. 392, pp. 1167–1202, 2025, doi: 10.1007/s00208-024-03084-4.

[16] D. G. Cantor, "Computing in the Jacobian of a hyperelliptic curve," *Mathematics of Computation*, vol. 48, no. 177, pp. 95–101, 1987, doi: 10.1090/S0025-5718-1987-0866101-0.

[17] E. W. Howe, E. Nart, and C. Ritzenthaler, "Jacobians in isogeny classes of abelian surfaces over finite fields," *Annales de l'Institut Fourier*, vol. 59, no. 1, pp. 239–289, 2009, doi: 10.5802/aif.2430.

[18] R. Bröker, E. W. Howe, K. E. Lauter, and P. Stevenhagen, "Genus-2 curves and Jacobians with a given number of points," *LMS Journal of Computation and Mathematics*, vol. 18, pp. 170–197, 2015, doi: 10.1112/S1461157014000461.

[19] D. Boneh, "Finding smooth integers in short intervals using CRT decoding," *Journal of Computer and System Sciences*, vol. 64, no. 4, pp. 768–784, 2002, doi: 10.1006/jcss.2002.1827.

[20] K. Bringmann, "A near-linear pseudopolynomial time algorithm for subset sum," in *Proceedings of the Twenty-Eighth Annual ACM–SIAM Symposium on Discrete Algorithms (SODA 2017)*, 2017, pp. 1073–1084. doi: 10.1137/1.9781611974782.69.

[21] J. C. Lagarias and A. M. Odlyzko, "Solving low-density subset sum problems," *Journal of the ACM*, vol. 32, no. 1, pp. 229–246, 1985, doi: 10.1145/2455.2461.

[22] M. Hittmeir, "Smooth subsum search: a heuristic for practical integer factorization." 2023.