FLOORS FOR DETERMINISTIC INTEGER FACTORING: COVERING MODELS, PARTIAL INFORMATION, THE ADDITIVE STRUCTURE OF THE LEHMAN–HARVEY START SET, AND THREE FURTHER FLOORS

SEAN WARD AND MAESTRO

Abstract. The fastest proven deterministic factoring algorithm for a balanced semiprime $N = pq$ runs in $N^{1/5+o(1)}$ operations, and Harvey's question whether the search over Lehman's $N^{1/3}$ candidates can reach $N^{1/6}$ is open. This report defines a covering model that contains Harvey's algorithm exactly and, up to factors $N^{o(1)}$, those of Lehman and Harvey–Hittmeir, and proves its floors: $N^{1/3}$ candidates, $N^{1/5}$ with materialised giants, $N^{1/6}$ with free giants. The exponents persist for $p \geq N^{2/5}$, the first two against fixed-degree forms and adaptive cell queries respectively, and thinning by a residue hypothesis modulo $\mathsf{q} \leq N^{1/20}$ buys at most a power of $\log\log N$. Given an interval of length $L = N^{\lambda}$ containing p, a localised search costs $N^{o(1)}L^{3/5}N^{-1/10}$, matching the model's floor for $\lambda \geq 3/8$; for $N^{1/6} \ll L \leq N^{3/8}$ the in-model cost is classified by the interval's Diophantine depth; a known residue $p \bmod M$, $M \leq N^{1/7}$, gives $N^{1/5+o(1)}M^{-2/5}$. In the explicit-difference model an $N^{1/6}$ search needs a difference cover, and the additive structure of the window starts governs every such cover: proved lower bounds $r^{1/3}$ (modulus-free) and $N^{1/12}$ (at $r = N^{1/3}$; for the squarefree shell, for almost all N) against upper bounds $2.1\,r^{2/3}$ and $6N^{2/9}$, with the envelope problem open. Further, a common factor $g = N^{\gamma}$ of $p-1$ and $q-1$ lets N be factored deterministically from N alone below $N^{1/5}$ for every $\gamma > 1/20$, by composing McKee–Pinch's progression search, made deterministic, with Pollard–Strassen on $N-1$ and Harvey–Hittmeir's order selection; a fixed list of elliptic curves factors every product of two primes from a range once its exposure labels separate, with computed separating lists for three dyadic ranges below 2^{23}; and NFS polynomial selection has a random-root floor $N^{1/(d+1)-o(1)}$, a rigorous resultant floor and, under a stated counting heuristic, no room to move the GNFS constant. Every rigorous floor is a theorem inside a stated model, the heuristic optima are labelled as such, and nothing here is a lower bound on factoring.

Contents

Date: 2 September 2026.

small and then θ with $1/(2\sqrt{e}(1-\varepsilon)) < \theta < 1/(2\sqrt{e})+2\delta$, Proposition 35.3 says that on a positive relative proportion of the corresponding nearly balanced semiprimes a plain algorithm from 1974 provably succeeds within $O(N^{1/(4\sqrt{e})+\delta})$ modular multiplications. It is not an improvement of the worst-case guarantee, and a fallback to Harvey's algorithm on the failures leaves the expected cost at $N^{1/5+o(1)}$. The record smoothness thresholds would formally lead to exponents $0.2961/2 = 0.14805$ and $0.2844/2 = 0.1422$, each with a positive slack; the theorems behind them do not give a positive proportion. If the available smooth-prime count is $\gg x/(\log x)^C$, the same pairing gives $\gg x^2/(\log x)^{C+1}$ products, a relative proportion $\gg (\log x)^{1-C}$ of the family; an infinitude theorem gives infinitely many such products. (e) The fixed-θ run does not factor almost all semiprimes of the family: after removing the $o(\pi(x))$ small-order exceptions Ω, the Fouvry set still contains a positive proportion of primes q with $q \nmid 2^E - 1$, and pairs of two such primes form a positive proportion on which $g = 1$. More generally, fix $\eta \in (0, \varepsilon)$ with $0.66 < \alpha(1-\eta)$ and let $G_\eta := \{q \in (x^{1-\eta}, x] : P^+(q-1) \geq q^\alpha\} \setminus \Omega$, still a positive proportion of the primes of the family. For $q, r \in G_\eta$ and $N = qr \leq x^2$, every $B, B_2 \leq N^{0.33} \leq x^{0.66} < x^{\alpha(1-\eta)} < q^\alpha \leq P^+(q-1)$; if the stage-1 exponent has prime support at most B then $\mathrm{ord}_q(2) \nmid Ev$ for every $1 \leq v \leq B_2$ (otherwise $P^+(q-1) \nmid \mathrm{ord}_q(2)$, forcing $\mathrm{ord}_q(2) < q^{1-\alpha} \leq x^{1-\alpha}$, contrary to $q \notin \Omega$), and likewise for r. So pairs from G_η form a positive relative proportion on which the single-exponent base-2 $p-1$ method, with any stage-1 and stage-2 bounds up to $N^{0.33}$, returns no factor: a limitation of that method, not a lower bound for all algorithms of that cost.

36. Open problems

Prove or break Conjecture 33.1 for an explicit curve family, including uniform control as u grows; find a separating family with per-member success rate near $1/2$ and an alphabet richer than the residual order; determine whether the separation tail structured by $p \bmod 3$ can be removed by mixing families; and prove a positive-proportion theorem for shifted primes $p - 1 = (x^\theta\text{-smooth}) \times (\text{prime} \leq x^{2\theta})$ below $\theta = 1/(2\sqrt{e})$, which would lower the exponent of Proposition 35.3. Any of the first three could change constants or coverage; heuristically, an exponent change requires leaving the smooth-order paradigm.

Reproducibility. The label statistics of Table 12 are exact computations on the full prime populations of the stated intervals, by adaptive refinement of the label partition as described in Section 33.3; the tests of Section 34 and the $p-1$ samples of remark (b) use pseudorandom populations from a seeded generator (seeds 3, 9 and 11 respectively) and are reproducible from those seeds; the counted multiplications and curve counts are deterministic; the wall-clock times and peak memory figures are single measurements on one machine and are reported as such. The code and the archived outputs are in the repository [23].

Part 6. Coefficient floors of number-field-sieve polynomial selection

Summary. Polynomial selection for the number field sieve chooses a polynomial f of degree d and a root m of f modulo N; in the unskewed model the sieve's figure of merit is the norm product $P = \|f\|_\infty m$, and this part asks how small it can be made. For a fixed root the coefficient vectors form a lattice of determinant N, so a polynomial with $\|f\|_\infty \leq N^{1/(d+1)}$ exists, and for a random root of a balanced semiprime $N^{1/(d+1)-o(1)}$ is a proven floor. When the root is free, a counting heuristic puts the minimum of P at $N^{(2d-1)/(d^2+d-1)}$, below the scale $N^{2/(d+1)}$ of the base-m and Kleinjung constructions, and complete enumerations at small sizes fit that exponent at $d = 2$ and $d = 3$. For two polynomials with a common root the resultant gives the rigorous floor $\|f\|_\infty^e \|g\|_\infty^d \gg N$, and a count of the pairs with a common root modulo a generic N gives, within the standard heuristic optimisation, the existence bound $\alpha\delta \geq 2 - o(1)$ for the two-polynomial dial: the GNFS constant 1.923 is then its existence optimum, and

the SNFS constant is out of reach for generic N at every pair of degrees. The room below the base-m scale is lower order in L-notation, and reaching it by search is estimated to cost a fractional power of N in trials: the floor asks for an algebraic small-coefficient method, not search. The rigorous content is the two floors; the rest is heuristic, with its finite verification stated as such.

37. Introduction

The general number field sieve [53, 9] factors N in heuristic time $L_N[1/3, (64/9)^{1/3}]$ with $L_N[s,c] = \exp((c+o(1))(\ln N)^s(\ln\ln N)^{1-s})$. Its polynomial selection step chooses $f \in \mathbb{Z}[x]$ of degree d with a root m modulo N; the sizes of $\|f\|_\infty$ and m enter the exponent through the norm product, and in practice through Murphy's E-value, skew, rotation and root properties [62, 45, 6]. This part isolates the size question – how small can $\|f\|_\infty$ and m be made jointly, and what is the consequence for the constant c – and answers it with two proven floors, one heuristic floor checked by exact enumeration, one classical identity read as a search problem, and one heuristic optimisation. Throughout, $\|f\|_\infty := \max_i |f_i|$ is the largest absolute value of a coefficient of $f = \sum_i f_i x^i$, and N is called *generic* when the counting heuristic of Proposition 39.1 – roots of bounded polynomials equidistributed modulo N – is assumed for it. The asymptotic conclusion, within the two-polynomial heuristic model developed here, is negative and quantified: coefficient size does not change the constant $(64/9)^{1/3}$ for generic N, and any remaining gain from polynomial selection is lower order. In numbers: the random-root floor is $N^{1/(d+1)-o(1)}$ (Proposition 38.1); the joint heuristic floor $N^{(2d-1)/(d^2+d-1)}$ is matched by exact enumerations with fitted exponents 0.607 ± 0.009 at $d=2$ (predicted 0.6) and 0.460 ± 0.014 at $d=3$ (predicted 5/11); the resultant floor $\|f\|_\infty^e\|g\|_\infty^d \gg N$ together with the heuristic count of pairs with a common root gives $\alpha\delta \geq 2 - O(1/(d+e))$ for generic N, hence the GNFS constant 1.923 as the existence optimum and not the SNFS constant 1.526; for degree two, selection is a bounded near-square search whose event counts are consistent with a Poisson model; and the gap between the joint floor and the base-m scale is 9–24 bits in the norm product at 512–1024 bits for $d = 5, 6$, which direct search would need about $N^{0.09}$–$N^{0.10}$ trials to cross and $N^{0.12}$–$N^{0.14}$ to reach the floor.

38. The fixed-root lattice

For a residue m let $L_{N,m} = \{(f_0,\dots,f_d) \in \mathbb{Z}^{d+1} : \sum_i f_i m^i \equiv 0 \pmod N\}$, the kernel of $(f_i) \mapsto \sum f_i m^i \bmod N$, a lattice of determinant N.

Proposition 38.1. *(i) $L_{N,m}$ contains a nonzero vector of sup-norm $\leq N^{1/(d+1)}$. (ii) Let $N = pq$ with distinct primes p, q, and let $H < \min(p,q)$. For m uniform on $\mathbb{Z}/N$,*

$$\Pr[\exists f \neq 0,\ \|f\|_\infty \leq H,\ f(m) \equiv 0 \pmod N] \leq d^2(2H+1)^{d+1}/N,$$

so, when $\min(p,q) \geq N^{1/(d+1)}$ – in particular for balanced semiprimes – for every fixed $\varepsilon > 0$ the shortest vector at random m has sup-norm $\geq N^{1/(d+1)-\varepsilon}$ with probability at least $1 - d^2 3^{d+1} N^{-\varepsilon(d+1)}$.

Proof. (i) is Minkowski on the cube. (ii): a nonzero f with $\|f\|_\infty \leq H$ is nonzero modulo p and modulo q, hence has at most d roots modulo each and at most d^2 modulo N by the Chinese remainder theorem ($x^2 - 1$ attains four); there are fewer than $(2H+1)^{d+1}$ such f. □

The Minkowski vector represents a nonzero polynomial of degree at most d; exact degree, irreducibility and usability for the sieve are not asserted. Exact Euclidean shortest-vector lengths (LLL-seeded Fincke–Pohst enumeration in dimension $d+1 \leq 7$), normalised by $N^{1/(d+1)}$ and averaged over 20 balanced semiprimes ($q/p < \sqrt{2}$) per size at 64, 96 and 128 bits, are 0.62–0.80 for random m, matching the Gaussian-heuristic constants $V_n^{-1/n}$, V_n the volume of the

Euclidean unit ball in $\mathbb{R}^n$ (0.62–0.80 for $n = 3, \dots, 7$). For the base-m choice $m = \lfloor N^{1/d} \rfloor$, simultaneous Dirichlet approximation of $r/m, \dots, r/m^{d-1}$ with $r = N - m^d$ gives vectors of sup-norm $O_d(N^{(d-1)/d^2})$, a ratio $N^{-1/(d^2(d+1))}$ to the generic fixed-root scale $N^{1/(d+1)}$ that predicts the measured change of the ratio from 64 to 128 bits ($0.291, 0.574, 0.839$ predicted against $0.30, 0.56, 0.84$ measured for $d = 3, 4, 6$); for special $N = 2^k - c$ the lattice contains $2^s x^d - c$ and the ratio collapses.

39. The joint floor

When the root is free, the figure of merit is $P(f, m) = \|f\|_\infty m$, where for a nonzero residue root r we put $m := \min(r, N - r) \in [1, N/2]$ and, replacing $f(x)$ by $f(-x)$ when $r > N/2$ (which preserves $\|f\|_\infty$), assume $f(m) \equiv 0 \pmod N$ (the root 0 is excluded, since $x^d + N$ has $P = 0$). Throughout, the admissible polynomials are those of exact degree d, irreducible over $\mathbb{Q}$ (the content is not restricted; every minimiser found below is primitive), with a nonzero root modulo N; $f(m)$ may be any nonzero multiple of N, and $\|f\|_\infty$ is the largest absolute value among all $d + 1$ coefficients.

Proposition 39.1 (heuristic)**.** *Let $N = pq$ be generic and $d \geq 2$. Among irreducible f of degree d with a nonzero root modulo N,*

$$\min P(f, m) = N^{(2d-1)/(d^2+d-1)+o(1)}, \qquad \|f\|_\infty = N^{(d-1)/(d^2+d-1)+o(1)}, \quad m = N^{d/(d^2+d-1)+o(1)}$$

at the minimiser.

Derivation. There are two constraints. (i) Counting: the number of polynomials with $\|f\|_\infty \leq H$ is $\asymp H^{d+1}$; a polynomial has on average one root modulo N, and the roots are assumed equidistributed, so the number of pairs with $m \leq M$ is $\asymp H^{d+1}M/N$; existence requires $(d + 1) \log_N H + \log_N M \geq 1$. (ii) Nontriviality: an irreducible f has $f(m) \neq 0$, so $|f(m)| \geq N$ and $(d + 1)\|f\|_\infty m^d \geq N$. Minimising $\log_N H + \log_N M$ on this polyhedron gives the vertex $((d - 1)/(d^2 + d - 1), d/(d^2 + d - 1))$. Constraint (ii) is a theorem and gives the rigorous $P \geq (N/(d + 1))^{1/d}$; constraint (i) is the heuristic. □

The three construction regimes in this measure are: Dirichlet vectors at $m = N^{1/d}$, $P = N^{(2d-1)/d^2}$; base-m and Kleinjung's regime $\|f\|_\infty \approx m \approx N^{1/(d+1)}$, $P = N^{2/(d+1)}$; and the joint floor $N^{(2d-1)/(d^2+d-1)}$ – $N^{0.75}, N^{0.667}, N^{0.6}$ at $d = 2$ and $N^{0.36}, N^{0.333}, N^{0.310}$ at $d = 5$ (the balanced base-m expansion attains the scale $N^{2/(d+1)}$ without the irreducibility requirement, and the constructions of [45] attain it in practice). The gap between the last two is $N^{(d-1)/((d+1)(d^2+d-1))}$, lower order in L-notation: about 9–24 bits of norm product at 512–1024 bits for $d = 5, 6$.

Refined count. After imposing the leading-term cutoff $m \gtrsim (N/f_d)^{1/d}$ and quotienting by mirror orbits, the expected number $\Lambda_d(x)$ of pairs with $P \leq x$ is a finite sum over coefficient shells whose leading term is $\frac{2}{3}x^5/N^3$ ($d = 2$) and $\frac{16}{15}x^{11/2}/N^{5/2}$ ($d = 3$); under a Poisson model with these intensities $\mathbb{E}P_{\min} = 0.996\, N^{3/5}$ and $0.912\, N^{5/11}$.

Complete enumeration. Using the known factorisation, the exact minimum of P over the admissible polynomials was computed by complete enumeration (square-root tables modulo p, q for $d = 2$, value tables for $d = 3$); the pruning bounds are exact consequences of $|f(\pm m)| \geq N$, the enumeration checks at run time that its finite search windows were not exceeded, and the routine is checked against brute force on small moduli in the accompanying test suite. For 51 balanced semiprimes at 24–44 bits ($d = 2$) the ordinary least-squares slope of $\log_2 P_{\min}$ on $\log_2 N$ is 0.6067 ± 0.0088 (predicted 0.6); for 42 distinct moduli among 44 generated instances at 16–32 bits ($d = 3$) it is 0.4603 ± 0.0137 (predicted $5/11 = 0.4545$; 0.4595 ± 0.0131 with the two duplicated moduli counted twice). The base-m control – one balanced expansion per N

at $m = \lceil N^{1/(d+1)} \rceil$ with $f(m) = N$, not restricted to irreducible f – fits 0.6669 against 2/3 and 0.5037 against 1/2. The row means of the coefficient and root exponents are 0.18–0.20 and 0.40–0.41 ($d = 2$) and 0.13–0.17 and 0.28–0.29 ($d = 3$); individual instances spread more widely. The ratio $P_{\min}/\mathbb{E}P_{\min}$ ranges over 0.70–1.09 rowwise; under the Poisson model $\Lambda_d(P_{\min})$ should be exponential with mean one, and it has mean 0.67 and 0.49 (Kolmogorov–Smirnov $p = 0.048$ and 0.001 on the generated instances): the model is borderline for $d = 2$ and rejected for $d = 3$, the minima lying below its prediction. A search through $8N^{(d-1)/(d^2+d-1)}$ leading coefficients (two adjacent candidate bases per leading coefficient, balanced lower digits, irreducible results only) found 50/51 and 37/44 exact minima; in the cubic case the mean excess was 0.070 bits – finite evidence for the predicted search scale, not an asymptotic search theorem.

40. Two polynomials: the resultant floor

Proposition 40.1. *Let $f, g \in \mathbb{Z}[x]$ be coprime over $\mathbb{Q}$, of degrees d, e, with a common root modulo each prime dividing squarefree N. Then $N \mid \operatorname{Res}(f, g)$ and*

$$N \le |\operatorname{Res}(f,g)| \le \|f\|_2^e \, \|g\|_2^d \le (d+1)^{e/2}(e+1)^{d/2}\|f\|_\infty^e \|g\|_\infty^d.$$

In particular two quadratics with a common root modulo N satisfy $\|f\|_\infty \|g\|_\infty \ge \sqrt{N}/3$.

Proof. $\operatorname{Res}(f, g) = Af + Bg$ with $A, B \in \mathbb{Z}[x]$ (adjugate of the Sylvester matrix), so a common root modulo p gives $p \mid \operatorname{Res}$; coprimality makes the resultant nonzero; Hadamard's inequality on the Sylvester matrix gives the norm bounds. □

Montgomery's two-quadratics construction [61], as described in [62], produces pairs at this floor up to a constant factor for the N to which it applies. For the usual linear side $g = x - m$ the inequality is $\|f\|_\infty m^d \gg_d N$, the nontriviality constraint of Proposition 39.1. The inequality is standard; its reading as a coefficient floor for nonlinear pairs is the point here. Exact (d, d) floors – complete enumeration over primitive, coprime, irreducible pairs of exact degree d with a nonzero common root, on 18 moduli at 16–28 bits ($d = 2$) and 21 moduli at 16–24 bits ($d = 3$) – give $P_2 = \|f\|_\infty \|g\|_\infty$ at 1.4–1.9 times the resultant lower bound $N^{1/d}/(d + 1)$, with fitted slopes 0.482 ± 0.005 ($d = 2$) and 0.313 ± 0.015 ($d = 3$) approaching $1/d$ from below; 16 of the 21 cubic minimisers have a monic side of sup-norm 1, whose partner is a short vector of the product of the two prime ideals of $\mathbb{Z}[\alpha]$ determined by the chosen modular roots, α a root of the monic side, and that "tiny-f" route has fitted exponents $0.5004, 0.3332, 0.2483$ for $d = 2, 3, 4$ on 33, 34 and 41 moduli at 24–96 bits, agreeing with $1/d$ to three decimal places. Under the balanced-minima heuristic for the orthogonal lattice, the constructible geometric-progression pairs [61, 47, 70, 18] (root-lift of a d-th root of N modulo a prime $p' \approx N^{1/d}$, orthogonal lattice of determinant $\approx N^{1-1/d}$) are predicted to reach only $P_2 \approx N^{2(d-1)/d^2}$ (measured slopes 0.4991 ± 0.0018, 0.4493 ± 0.0030, 0.3744 ± 0.0034 on ten moduli at each of $40, 64, 96, 128$ bits, against $0.5, 0.444, 0.375$), which equals the floor only at $d = 2$.

41. Degree two: a bounded near-square search

Lemma 41.1 (bridge)**.** *Let $f = ax^2 + bx + c \in \mathbb{Z}[x]$, $a > 0$, and $f(m) = kN$ with $k \ne 0$; put $y = 2am + b$. Then $y^2 - 4akN = b^2 - 4ac = \operatorname{disc} f$. Conversely, given (a, k, y) and $b \equiv y \pmod{2a}$, the integers $m = (y - b)/(2a)$ and $c = (b^2 - (y^2 - 4akN))/(4a)$ satisfy $f(m) = kN$. If $\|f\|_\infty \le H$ then $|\operatorname{disc} f| \le 5H^2$, sharp at $(H, H, -H)$.*

Proof. $(2am + b)^2 = 4a(am^2 + bm + c) + b^2 - 4ac = 4akN + \operatorname{disc} f$. Conversely $b \equiv y \pmod{2a}$ gives $b^2 \equiv y^2 \pmod{4a}$, so $c \in \mathbb{Z}$ and substitution gives $f(m) = kN$; the discriminant bound is $|b^2 - 4ac| \le H^2 + 4H^2$. □

The pairs (f, m) with $a > 0$ therefore correspond bijectively to quadruples (a, k, y, b) with $b \equiv y \pmod{2a}$; the choice of b within its class selects a translate $f(x + t)$, which preserves y. A bounded known-root quadratic is a near-square $4akN = y^2 - \Delta$ with $|\Delta| \le 5H^2$, and at the joint floor $H = N^{1/5}$ degree-two selection is the search for $a \le N^{1/5}$ and a bounded multiplier k with $4akN$ within $O(N^{2/5})$ of a square, plus a congruent representative passing the coefficient filters (the near-square condition is necessary, not sufficient). The identity is classical (Lehman [49], MPQS's $(ax + b)^2 - N = aQ(x)$ [77], Montgomery [61]); Harvey's deterministic algorithm [31] shares the multiplier exponent $N^{1/5}$ and the identity $U^2 - 4abN = v^2$ but requires a square residual, where selection needs only a small one. The expected number of bounded $k = 1$ pairs is $\lambda(H) \approx 4H^{5/2}/\sqrt{N}$ under equidistributed phases, the finite sum behind this leading term being what the computation predicts. For 200 balanced semiprimes at each of $40, 56, 72, 80$ bits, exhaustive enumeration through the bridge at $H = CN^{1/5}$, $C = 0.75, 1, 1.5$, gives pair means within 10% of the finite-sum prediction in 8 of the 12 (size, C) cells, within 12% in three more, and 25% below it at $C = 0.75$ and 56 bits; at $C = 1$ the observed means are 3.5–4.3 against the predicted 3.8–4.0. The pair variance is about ten times the mean, because translates and scalings $(at^2, yt, \Delta t^2)$ are exact dependencies; the scaling-primitive classes have variance approximately equal to the mean, and their means reproduce the zero fractions through $e^{-\mu}$ to within 0.024 – consistent with a Poisson model once the two dependencies are removed, a diagnostic rather than a goodness-of-fit test. The chirp phases $(y^2 - 4aN)/(2y)$ are consistent with a uniform uncorrelated null (variance 0.0830 against $1/12 = 0.0833$; pooled Kolmogorov–Smirnov $p = 0.21$ on 50 phases per modulus treated as independent, again a diagnostic; lag-one correlation 0.000 ± 0.004). Among the moduli with at least one $k = 1$ candidate at $C = 1.5$ (784 of the 800), the best $k = 1$ product has median 0.93–0.98 $N^{3/5}$ from 40 to 80 bits, an upper bound at the scale of the exact minima for those moduli.

42. The constant dial

Write the norm product of a two-polynomial relation scheme, up to lower-order factors, as $X = N^{\alpha/d} A^{\delta d}$: α is the N-content the pair carries per unit $1/d$ and δ the growth of the norm product per unit degree. Minimising $\ln X$ over d gives $\ln X = 2\sqrt{\alpha\delta \ln N \ln A}$; with A^2 candidate pairs (a, b), $|a|, |b| \le A$, Dickman smoothness with independent sides, a smoothness bound B and B^2 linear algebra, the usual balance gives

$$c(\alpha\delta) = \Big(\frac{32\,\alpha\delta}{9}\Big)^{1/3}$$

for the constant of $L_N[1/3, c]$ – 1.923 at $\alpha\delta = 2$ (GNFS: $\|f\|_\infty \approx m \approx N^{1/(d+1)}$, $\alpha = 2$, $\delta = 1$) and 1.526 at $\alpha\delta = 1$ (SNFS: $\|f\|_\infty = O(1)$, $m = N^{1/d}$). With A^t candidates the balance gives $c_t = (64\alpha\delta/(9t))^{1/3}$; if a t-dimensional sieve carries N-content $\alpha = 2(t - 1)$ – the value obtained by extrapolating the two-polynomial count, an assumption we do not derive – then $c_t = (128(t - 1)/(9t))^{1/3}$ is minimal at $t = 2$ within this model. The model is heuristic and calibrated on the two known constants.

Proposition 42.1 (the floor of the dial)**.** *Let f, g be coprime of degrees $d \ge e \ge 1$ with a common root modulo N, $F = \ln\|f\|_\infty$, $G = \ln\|g\|_\infty$, $L = \ln N$, so that $\alpha = d(F + G)/L$ and $\delta = (d+e)/d$. (i) Proposition 40.1 gives $eF + dG \ge L - O_{d,e}(1)$, hence $F + G \ge L/d - O(1)$ and*

$$\alpha\delta \;\ge\; 1 + \frac{e}{d} - O_{d,e}\Big(\frac{1}{L}\Big).$$

(ii) [heuristic] For generic N, the number of pairs with $\|f\|_\infty \le e^F$, $\|g\|_\infty \le e^G$ and a common root is about $e^{(d+1)F+(e+1)G}/N$, so existence needs $(d + 1)F + (e + 1)G \ge L$; minimising $F + G$

under (i) and (ii) gives $F+G = 2L/(d+e+1)$ for $e < d$ (at the vertex $F = L(d-e-1)/(d(d+1)-e(e+1))$, $G = L(d-e+1)/(d(d+1)-e(e+1))$) and L/d for $e = d$, hence

$$\alpha\delta \;\geq\; \frac{2(d+e)}{d+e+1} - o(1) \quad (e<d), \qquad \alpha\delta \geq 2 - o(1) \quad (e=d).$$

Consequences, within this heuristic model. For generic N the existence optimum of the two-polynomial dial is $\alpha\delta = 2 - o(1)$, i.e. $c = (64/9)^{1/3}$: GNFS's constant is optimal among two-polynomial relation schemes, and the room below it – the joint floor of Proposition 39.1 ($\alpha\delta = (2d-1)(d+1)/(d^2+d-1) \to 2$), non-monic linear sides ($2(d+1)/(d+2)$), skew – is lower order. The SNFS constant requires $\alpha\delta = 1 + o(1)$, which generic N does not admit at any pair of degrees; special N realise it through $f(m) = kN$ with $\|f\|_\infty = O(1)$. A modular root of a bounded polynomial buys only a (d,d) pair at the resultant floor through the ideal lattice, with $\alpha\delta = 2$ – a tie with GNFS (the (d,d) pair at its floor has the norm product $N^{1/d}A^{2d} = N^{2/D}A^D$ with $D = 2d$, that of a linear pair at base-m scale with degree parameter D), and the geometric-progression pairs have $\alpha\delta \to 4$, $c = 2.423$, worse. Constant-level gains for generic N must come from outside the two-polynomial dial – side multiplicity (Coppersmith's multiple-polynomial NFS [16], 1.902) and amortisation (Coppersmith's factory [16], 1.639 per target after a shared 2.007 precomputation) – or from outside the relation paradigm.

The free-root frontier (heuristic). Searching T leading coefficients $a_d = 1, \ldots, T$ with $m \approx (N/T)^{1/d}$ and balanced lower digits, the best of T trials has $P(T) \approx \max(T, (m/2)T^{-1/(d-1)})\, m$, which crosses the base-m scale $N^{2/(d+1)}$ at $T_\times = N^{2(d-1)/((d+1)(3d-2))}$ and reaches the joint floor at $T = N^{(d-1)/(d^2+d-1)}$. On three balanced semiprimes per size ($d = 3$ at 48–96 bits, $d = 4$ at 64–128 bits, budgets T checked at the powers of two up to $T_{\max} = 2^{18}$), six of the seven measured crossovers lie within one bit of the prediction and the seventh ($d = 4$, 128 bits) came 1.3 bits earlier; the theory curve is within 0.5 bits of the measured minimum at every crossover, and in the six rows with $T_{\max} \geq N^{(d-1)/(d^2+d-1)}$ the measured minimum ends 0.1–0.5 bits below the predicted floor, the formula continuing to fall past the floor while the measurement stops there. Heuristic extrapolation to NFS sizes puts the crossover budget at 2^{46}–2^{105} trials and the floor 2^{62}–2^{141} for $d = 5, 6$ at 512–1024 bits: realising the joint floor appears to require an algebraic method that makes $d-1$ base-m digits small at a free root, rather than direct search; within the dial, the resulting gain is lower order and does not change c.

43. What is open

The open questions are whether the joint floor can be reached in polynomial time (an algebraic small-digit selection); whether balanced (d,d) pairs at the resultant floor exist without a tiny-polynomial root (the counting heuristic predicts many); and, outside this part, whether any relation source has norms that do not carry $N^{\Theta(1/d)}$ per side while growing like $A^{\Theta(d)}$ – within the heuristic framework used here, the only place where the exponent $1/3$, rather than its constant, could move.

Reproducibility. Every number above is the output of a deterministic computation from the stated parameters: exact shortest-vector lengths, complete enumerations of the exact minima with pruning bounds derived from $|f(\pm m)| \geq N$ (checked against brute force on small moduli in the accompanying test suite), exhaustive enumeration through the bridge, and the coefficient search, on populations of balanced semiprimes ($q/p < \sqrt{2}$) drawn from a seeded generator (seeds 97, 111, 5, 131 and 23 for the fixed-root, single-polynomial, two-polynomial, bridge and frontier computations). Methods: all enumerations and root tests are in exact integer arithmetic; the reported slopes are ordinary least-squares fits of $\log_2 P_{\min}$ against $\log_2 N$ with the slope's standard error from the residuals; the Poisson checks compare the empirical distribution of

$\Lambda_d(P_{\min})$ with the exponential law of mean one by the Kolmogorov–Smirnov statistic and its asymptotic p-value; all statistics are in double precision. The code and the archived outputs accompany the paper.

References

[1] L. M. Adleman, Two theorems on random polynomial time, *Proc. 19th IEEE Symp. Foundations of Computer Science* (1978), 75–83.

[2] D. Aggarwal, U. Maurer, Breaking RSA generically is equivalent to factoring, *Advances in Cryptology – EUROCRYPT 2009*, LNCS 5479, Springer, 2009, 36–53.

[3] E. Bach, R. Peralta, Asymptotic semismoothness probabilities, *Math. Comp.* 65 (1996), 1701–1715.

[4] R. C. Baker, G. Harman, Shifted primes without large prime factors, *Acta Arith.* 83 (1998), 331–361.

[5] P. T. Bateman, R. A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.* 16 (1962), 363–367.

[6] S. Bai, C. Bouvier, A. Kruppa, P. Zimmermann, Better polynomials for GNFS, *Math. Comp.* 85 (2016), 861–873.

[7] D. Boneh, G. Durfee, Y. Frankel, An attack on RSA given a small fraction of the private key bits, *Advances in Cryptology – ASIACRYPT '98*, LNCS 1514, Springer, 1998, 25–34.

[8] D. J. Bernstein, T. Lange, Computing small discrete logarithms faster, *Progress in Cryptology – INDOCRYPT 2012*, LNCS 7668, Springer, 2012, 317–338.

[9] J. P. Buhler, H. W. Lenstra, Jr., C. Pomerance, Factoring integers with the number field sieve, in *The development of the number field sieve*, LNM 1554, Springer, 1993, 50–94.

[10] R. P. Brent, Some integer factorization algorithms using elliptic curves, *Austral. Comput. Sci. Comm.* 8 (1986), 149–163 (reporting Suyama's parametrisation).

[11] D. A. Burgess, On character sums and primitive roots, *Proc. London Math. Soc.* (3) 12 (1962), 179–192.

[12] P. Bürgisser, On defining integers and proving arithmetic circuit lower bounds, *Comput. Complexity* 18 (2009), 81–103.

[13] N. A. Carella, Note: integer factoring methods III, arXiv:0707.4468 (2007); unrefereed.

[14] N. A. Carella, Deterministic integer factorization algorithms, arXiv:1308.2891 (2013); unrefereed.

[15] Q. Cheng, On the ultimate complexity of factorials, *Theoret. Comput. Sci.* 326 (2004), 419–429.

[16] D. Coppersmith, Modifications to the number field sieve, *J. Cryptology* 6 (1993), 169–180.

[17] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities, *J. Cryptology* 10 (1997), 233–260.

[18] N. Coxon, On nonlinear polynomial selection for the number field sieve, preprint, arXiv:1109.6398 (2011).

[19] I. Damgård, M. Koprowski, Generic lower bounds for root extraction and signature schemes in general groups, *Advances in Cryptology – EUROCRYPT 2002*, LNCS 2332, Springer, 2002, 256–271.

[20] N. D. Elkies, C. T. McMullen, Gaps in $\sqrt{n}$ mod 1 and ergodic theory, *Duke Math. J.* 123 (2004), 95–139.

[21] D. El-Baz, J. Marklof, I. Vinogradov, The two-point correlation function of the fractional parts of $\sqrt{n}$ is Poisson, *Proc. Amer. Math. Soc.* 143 (2015), 2815–2828.

[22] T. Estermann, Einige Sätze über quadratfreie Zahlen, *Math. Ann.* 105 (1931), 653–662.

[23] S. Ward, Maestro, *factorlab and latticelab*: code, tests and archived results behind the reports, version 2026.09, https://github.com/iGentAI/factorlab.

[24] M. Filaseta, O. Trifonov, On gaps between squarefree numbers II, *J. London Math. Soc.* 45 (1992), 215–221.

[25] É. Fouvry, Théorème de Brun–Titchmarsh; application au théorème de Fermat, *Invent. Math.* 79 (1985), 383–407.

[26] J. B. Friedlander, Shifted primes without large prime factors, in: *Number Theory and Applications* (Banff, 1988), NATO Adv. Sci. Inst. Ser. C 265, Kluwer, Dordrecht, 1989, 393–401.

[27] Y. Gao, Y. Feng, H. Hu, Y. Pan, On factoring and power divisor problems via rank-3 lattices and the second vector, Cryptology ePrint Archive 2025/1004; to appear in *Math. Comp.*

[28] R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete Mathematics*, 2nd ed., Addison-Wesley, 1994.

[29] S. D. Galbraith, J. M. Pollard, R. S. Ruprai, Computing discrete logarithms in an interval, *Math. Comp.* 82 (2013), 1181–1195.

[30] W. B. Hart, A one line factoring algorithm, *J. Aust. Math. Soc.* 92 (2012), 61–69.

[31] D. Harvey, An exponent one-fifth algorithm for deterministic integer factorisation, *Math. Comp.* 90 (2021), 2937–2950; arXiv:2010.05450.

[32] D. Harvey, M. Hittmeir, A log-log speedup for exponent one-fifth deterministic integer factorisation, *Math. Comp.* 91 (2022), 1367–1379; arXiv:2105.11105.

[33] D. Harvey, M. Hittmeir, Deterministic methods for finding elements of large multiplicative order, arXiv:2601.11131 (2026).
[34] D. R. Heath-Brown, Square-free values of n^2+1, *Acta Arith.* 155 (2012), 1–13.
[35] N. Heninger, H. Shacham, Reconstructing RSA private keys from random key bits, *Advances in Cryptology – CRYPTO 2009*, LNCS 5677, Springer, 2009, 1–17.
[36] M. Herrmann, A. May, Solving linear equations modulo divisors: on factoring given any bits, *Advances in Cryptology – ASIACRYPT 2008*, LNCS 5350, Springer, 2008, 406–424.
[37] M. J. Hinek, Another look at small RSA exponents, *Topics in Cryptology – CT-RSA 2006*, LNCS 3860, Springer, 2006, 82–98.
[38] M. J. Hinek, *On the security of some variants of RSA*, PhD thesis, University of Waterloo, 2007.
[39] M. Hittmeir, A babystep-giantstep method for faster deterministic integer factorization, *Math. Comp.* 87 (2018), 2915–2935.
[40] M. Hittmeir, A time-space tradeoff for Lehman's deterministic integer factorization method, *Math. Comp.* 90 (2021), 1999–2010.
[41] C. Hooley, On the power free values of polynomials, *Mathematika* 14 (1967), 21–26.
[42] N. Howgrave-Graham, Finding small roots of univariate modular equations revisited, *Cryptography and Coding*, LNCS 1355, Springer, 1997, 131–142.
[43] M. N. Huxley, *Area, Lattice Points, and Exponential Sums*, London Math. Soc. Monographs (N.S.) 13, Oxford University Press, 1996.
[44] A. Ya. Khinchin, *Continued Fractions*, University of Chicago Press, 1964.
[45] T. Kleinjung, On polynomial selection for the general number field sieve, *Math. Comp.* 75 (2006), 2037–2047.
[46] P. Koiran, Valiant's model and the cost of computing integers, *Comput. Complexity* 13 (2004), 131–146.
[47] N. Koo, G. H. Jo, S. Kwon, On nonlinear polynomial selection and geometric progression (mod N) for number field sieve, IACR Cryptology ePrint Archive, Report 2011/292 (2011).
[48] J. Kärkkäinen, P. Sanders, S. Burkhardt, Linear work suffix array construction, *J. ACM* 53 (2006), 918–936.
[49] R. S. Lehman, Factoring large integers, *Math. Comp.* 28 (1974), 637–646.
[50] H. W. Lenstra, Jr., Factoring integers with elliptic curves, *Ann. of Math.* 126 (1987), 649–673.
[51] J. D. Lichtman, Primes in arithmetic progressions to large moduli, and shifted primes without large prime factors, arXiv:2211.09641 (2022).
[52] R. J. Lipton, Straight-line complexity and integer factorization, *Algorithmic Number Theory (ANTS-I)*, LNCS 877, Springer, 1994, 71–79.
[53] A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, J. M. Pollard, The number field sieve, in *The development of the number field sieve*, LNM 1554, Springer, 1993, 11–42.
[54] H. W. Lenstra, Jr., C. Pomerance, A rigorous time bound for factoring integers, *J. Amer. Math. Soc.* 5 (1992), 483–516.
[55] C. Lutsko, A. Sourmelidis, N. Technau, Pair correlation of the fractional parts of αn^θ, arXiv:2106.09800 (2021).
[56] C. Lutsko, N. Technau, m-point correlations of the fractional parts of αn^θ, *Amer. J. Math.*, to appear.
[57] U. M. Maurer, Factoring with an oracle, *Advances in Cryptology – EUROCRYPT '92*, LNCS 658, Springer, 1993, 429–436.
[58] J. McKee, R. G. E. Pinch, Further attacks on server-aided RSA cryptosystems, manuscript, 1998. Its abstract (on the second author's publication page) states a method of cost $O(N^{1/4}/\beta)$ for moduli whose $p-1$ and $q-1$ share the factor β; the text itself we could not retrieve, and the statements used here are those restated in [38, §6.3].
[59] G. L. Miller, Riemann's hypothesis and tests for primality, *J. Comput. System Sci.* 13 (1976), 300–317.
[60] P. L. Montgomery, Speeding the Pollard and elliptic curve methods of factorization, *Math. Comp.* 48 (1987), 243–264.
[61] P. L. Montgomery, Small geometric progressions modulo n, unpublished note, 1993; see also the account in the thesis of Murphy above.
[62] B. A. Murphy, *Polynomial selection for the number field sieve integer factorisation algorithm*, PhD thesis, Australian National University, 1999.
[63] M. Nair, Power free values of polynomials, *Mathematika* 23 (1976), 159–183.
[64] A. K. Lenstra, H. W. Lenstra, Jr. (eds.), *The Development of the Number Field Sieve*, Lecture Notes in Math. 1554, Springer, 1993.
[65] I. Nir, Deterministically finding an element of large order in $\mathbb{Z}_n^*$, arXiv:2605.09592 (2026).
[66] K. K. Norton, Numbers with small prime factors, and the least kth power non-residue, *Mem. Amer. Math. Soc.* 106 (1971).

[67] Z. Oznovich, B. L. Volk, On deterministically finding an element of high order modulo a composite, *Proc. ACM-SIAM Symposium on Discrete Algorithms (SODA 2026)*, 6379–6391.
[68] J. M. Pollard, Theorems on factorization and primality testing, *Proc. Cambridge Philos. Soc.* 76 (1974), 521–528.
[69] J. M. Pollard, Theorems on factorization and primality testing, *Proc. Cambridge Philos. Soc.* 76 (1974), 521–528.
[70] T. Prest, P. Zimmermann, Non-linear polynomial selection for the number field sieve, *J. Symbolic Comput.* 47 (2012), 401–409.
[71] M. Radziwiłł, K. Shubin, Poissonian pair correlation for αn^θ mod 1, *Int. Math. Res. Not. IMRN* 2024, no. 9, 7654–7688.
[72] R. L. Rivest, A. Shamir, Efficient factoring based on partial information, *Advances in Cryptology – EUROCRYPT '85*, LNCS 219, Springer, 1986, 31–34.
[73] O. Robert, P. Sargos, Three-dimensional exponential sums with monomials, *J. reine angew. Math.* 591 (2006), 1–20.
[74] J. B. Rosser, L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* 6 (1962), 64–94.
[75] V. Shoup, Lower bounds for discrete logarithms and related problems, *Advances in Cryptology – EUROCRYPT '97*, LNCS 1233, Springer, 1997, 256–266.
[76] M. Shub, S. Smale, On the intractability of Hilbert's Nullstellensatz and an algebraic version of "NP $\neq$ P?", *Duke Math. J.* 81 (1995), 47–54.
[77] R. D. Silverman, The multiple polynomial quadratic sieve, *Math. Comp.* 48 (1987), 329–339.
[78] V. Strassen, Einige Resultate über Berechnungskomplexität, *Jber. Deutsch. Math.-Verein.* 78 (1976/77), 1–8.
[79] N. Technau, N. Yesha, On the correlations of n^α mod 1, arXiv:2006.16629 (2020).
[80] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, 3rd ed., Grad. Stud. Math. 163, Amer. Math. Soc., 2015.
[81] M. J. Wiener, Cryptanalysis of short RSA secret exponents, *IEEE Trans. Inform. Theory* 36 (1990), 553–558.

iGent AI
Email address: `sward@igent.ai`

iGent AI