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.

match, and Harvey's Algorithm 4.1 realised by a product tree and multipoint evaluation modulo N with the baby scan when the aggregate gcd is N – and run on 240 moduli $N = pq$ constructed as $p = 1 + kg$, $q = 1 + lg$ with $g = 2\ell$ for a prime ℓ, $\gcd(k, l) = 1$, $k < l < 2k$ (so $q/p < 2$), k and g each of about a quarter of the bits of N, and N of 36 to 44 bits, by rejection sampling from a seeded generator; the values of k ranged over $[259, 2014]$ and those of g over $[334, 2042]$. The size of k matters for the check: with k or l equal to 1 every non-liar base factors N at the immediate step $\gcd(\beta - 1, N)$ and the search never runs. All 240 moduli were factored, 239 of them by the collision search and one at the immediate gcd (a component order equal to 1); the base $\alpha = 2$ was a non-liar in every case, as expected since the liars form a subgroup of density $1/k$ modulo p. For the successful base the two component orders were recomputed from the known factors: the least exponent $e = \min(\mathrm{ord}_p\,\beta, \mathrm{ord}_q\,\beta)$ was at most 2014, and the ratio $e/(\sqrt{N}/g)$, which Lemma 26.2 bounds by 1, had maximum 0.9955 and mean 0.50 over the 239 collision cases, exceeding 0.9 in 21 of them. This checks the implementation and the inequality $e < \sqrt{N}/g$ on the tested population, not the asymptotics; the moduli, seed, per-modulus orders, exponents and search horizons are archived with the report.

Routes B and C of Section 28 were run, with g supplied, on 48 constructed balanced moduli of 33 to 56 bits with $\gcd(p - 1, q - 1) = N^\gamma$, $0.024 \le \gamma \le 0.312$, and the base $\alpha = 2$ (no baby collision occurred, so no other base was needed). Route B factored all 48, with babies plus giants between 1.01 and 1.92 times $\sqrt{n}$ on the 20 moduli with $n \ge 100$ candidates – an object count, not a count of bit operations – and Route C factored all 48 within n trials; 24 reruns with a proper common divisor in place of the gcd also factored their moduli. The recovery of g, the dovetailing and the order selection were not run; at these sizes they do not arise.

30. Where the class arises

The class of moduli with a large common factor is the exceptional set of a conditional procedure in Part 1, whose Proposition 7.3 states: for a balanced semiprime $N = pq$ that survives a Fermat preprocessing of $N^{1/6+o(1)}$ square tests, and under a uniform evaluation hypothesis of exponent γ for the interval sub-products of a certain product of $N^{1/3+o(1)}$ factors, a breadth-first bisection of that product factors N in $(1 + Z_*)N^{\gamma/3+o(1)}$ ring operations by trying the bases $\alpha = 2, 3, \ldots$ up to $(\log N)^4$, *unless* $\gcd(p - 1, q - 1) \ge N^{5/24}/(2\sqrt{C}(\log N)^3)$; here Z_* is a width parameter of that product. Lemma 26.2 and Corollary 27.1 dispose of the exception from N alone: every balanced semiprime with $g \ge N^{5/24}/(2\sqrt{C}(\log N)^3)$ is factored in $N^{7/48+o(1)}$ operations when $g \le (p-1)^{3/4}/(\log N)^3$ and in $O_{C,\varepsilon}(N^{1/(8\sqrt{\mathrm{e}})+\varepsilon})$ operations otherwise. Consequently a conditional algorithm of exponent t for the non-exceptional moduli extends to all balanced semiprimes with exponent $\max(t, 7/48)$ (up to $o(1)$), which equals t whenever $t \ge 7/48$; for a target exponent below $7/48$ the intermediate range $N^{5/24-o(1)} \le g \le (p-1)^{3/4}/(\log N)^3$ would contribute its $N^{7/48+o(1)}$ term, and the class needing separate treatment would be exactly that range.

Part 5. Exposure labels and finite separating certificates for a deterministic fixed-list elliptic curve method

Summary. For $N = pq$ with distinct odd primes p and q, a fixed list of elliptic curves, run with a stage-1 bound B_1 and an exact stage 2 to B_2, factors N as soon as one curve behaves differently modulo p and modulo q. We make this precise through an *exposure label* – for each curve and prime, the residual order of the stage-1 point if it is at most B_2, or one of three degenerate construction states, or no exposure – and prove that a curve factors N if and only if the two labels differ, so that distinct label vectors over a set of primes form a finite certificate that the list factors every product of two distinct primes from the set. Such certificates are computed for every prime of $[2^{18}, 2^{19})$, $[2^{20}, 2^{21})$ and

$[2^{22}, 2^{23})$ with ten, eleven and twelve Suyama curves. Under the conjecture that an explicit family separates in logarithmically many curves, the method with stage-1 bound $B_1 = x^{1/u}$ and $B_2 = B_1^2$ is a deterministic $N^{1/(2u)+o(1)}$ algorithm for products of two primes with bounded ratio; heuristically the route costs $L_N[1/2, 1] = \exp((1+o(1))\sqrt{\log N \log\log N})$ and cannot compete with the number field sieve. Unconditionally, Pollard's $p-1$ method with base 2 succeeds on a positive proportion of the semiprimes with both prime factors in $(x^{1-\varepsilon}, x]$, in $O_\theta(N^{\theta/2})$ multiplications for every $\theta > 1/(2\sqrt{\mathrm{e}})$ and small enough ε: a success theorem for a partial algorithm, not an improvement of any worst-case guarantee.

31. Introduction

The elliptic curve method [50] factors $N = pq$ when a random curve has a smooth order modulo one of the primes. It is analysed as a randomised algorithm for each target prime. Here we ask a different question: for a *fixed* list of curves, chosen without knowledge of N, which pairs (p, q) does the list factor, and how long must the list be to factor every pair of primes in a range? To our knowledge the best proven deterministic exponent is Harvey's $N^{1/5+o(1)}$ [31]; a fixed curve list with a logarithmic separating length would give, for semiprimes with bounded prime ratio, $N^{1/6+o(1)}$ at $u = 3$ by a mechanism unrelated to Harvey's, and N^ε for every fixed ε under the conjecture stated below. We are not aware of any asymptotic covering or separating theorem for an explicit fixed curve family of this kind, unconditionally or under GRH; the rigorous analyses of the elliptic curve method [50, 54] average over a random curve.

The observation that organises this part is that coverage is the wrong criterion. A curve that succeeds modulo both primes with the same residual order gives gcd $= N$; what factors N is a *difference* between the two primes' behaviour, and the right bookkeeping is a label per curve and prime fine enough that equal labels mean exactly "no one-sided relation".

The results are as follows. The label criterion (Proposition 32.4): a curve factors N if and only if the two labels differ, and a deterministic scan of the stage-2 atoms in key order may stop at the first two-sided atom. The finite certificates (Table 12): the first ten Suyama curves at $(B_1, B_2) = (64, 4096)$ separate every prime of $[2^{18}, 2^{19})$, the first eleven at $(102, 10321)$ every prime of $[2^{20}, 2^{21})$, and the first twelve at $(161, 26008)$ all 268 216 primes of $[2^{22}, 2^{23})$, while the collapsed binary signatures of the same predicate need 46–79 curves on the four smaller intervals and had not separated the largest after 40; at $u = 4$ ($B_1 = x^{1/4}$, $B_2 = x^{1/2}$) the separating lengths on all primes of $[x, 2x)$ are $31, 32, 36, 53$ at $x = 2^{16}, 2^{18}, 2^{20}, 2^{22}$, with coverage lengths $33, 35, 41, 53$. The implementation factors all 616 test pairs in at most three curves, and a counter of its ladder, differential-addition, inversion and product multiplications (the polynomial arithmetic excluded) has fitted exponent 0.175 against the predicted 1/6 up to logarithmic factors. Conjecture 33.1 (logarithmic separating length for an explicit family) gives the deterministic $N^{1/(2u)+o(1)}$ algorithm for bounded prime ratio and every fixed u; the route costs $L_N[1/2, 1] := \exp((1 + o(1))\sqrt{\log N \log\log N})$ heuristically; a non-uniform deterministic $L_N[1/2, 1]$ algorithm exists, and the two-sided degeneracy of the $p-1$ method is recovered by the binary Miller chain iff the 2-adic valuations of the two orders differ (Proposition 35.2). For a random list, pairwise separation in $O(\log x)$ curves follows from two-sided exposure-probability bounds with CRT independence and a Deuring–Lenstra anti-concentration estimate (Proposition 33.2); the content of the conjecture is explicitness. Finally, Proposition 35.3: for every $\theta \in (1/(2\sqrt{\mathrm{e}}), 1/2)$ and every $\varepsilon \in (0, 1/4)$ with $\theta(1-\varepsilon) > 1/(2\sqrt{\mathrm{e}})$, Pollard's base-2 $p-1$ method succeeds on a positive relative proportion of the semiprimes $N = pq$ with $x^{1-\varepsilon} < p, q \le x$ in $O_\theta(N^{\theta/2})$ modular multiplications, from the theorems of Friedlander and Fouvry on shifted primes; letting ε and the exponent slack tend to zero jointly gives exponents arbitrarily close to $1/(4\sqrt{\mathrm{e}}) = 0.151632\ldots < 1/5$.

32. Exposure labels

Fix $B_1 < B_2$ and let $L = \operatorname{lcm}\{\ell^e \le B_1\}$. For a Suyama parameter σ [10], the Montgomery curve [60] $By^2 = x^3 + Ax^2 + x$ with $a_{24} = (A+2)/4$ and its starting point are constructed from $U = \sigma^2 - 5$ and $V = 4\sigma$ through the denominator $16U^3V$; stage 1 computes $Q = [L]P$ on the x-line.

Definition 32.1 (exposure label)**.** For a prime p, set $\lambda_\sigma(p) = -1$ if $16U^3V \equiv 0 \pmod p$; otherwise set $\lambda_\sigma(p) = -2$ if $a_{24} \equiv 0 \pmod p$ and $\lambda_\sigma(p) = -3$ if $a_{24} \equiv 1 \pmod p$ (the curve $A = \mp 2$ is singular); otherwise set $\lambda_\sigma(p) = d$, the order of Q modulo p, if that order satisfies $d \le B_2$ (so $d = 1$ is a stage-1 success), and $\lambda_\sigma(p) = 0$ if the order exceeds B_2.

Proposition 32.2 (signatures factor pairs)**.** *Let $\mathcal{P}$ be a finite set of primes and $A_1, \dots, A_K$ deterministic ring computations such that if A_i succeeds modulo exactly one of p, q then its gcd step factors $N = pq$; write $s_i(p) = 1$ if A_i succeeds modulo p and $s_i(p) = 0$ otherwise, and $s(p) := (s_i(p))_{i \le K} \in \{0,1\}^K$. If the signatures $s(p)$ are distinct for every pair of distinct primes $p, q \in \mathcal{P}$, then the K computations factor every pq with distinct $p, q \in \mathcal{P}$ (a perfect-square test handles $p = q$; a computation that succeeds modulo both primes returns* $\gcd = N$ *and is passed over). Coverage is neither necessary nor sufficient for this.*

Proof. Distinct signatures supply an i with $s_i(p) \ne s_i(q)$, hence a one-sided gcd. A set in which one prime has the all-zero signature and all others are distinct is separated but not covered; two primes with the same nonzero signature are covered but not separated. □

Remark 32.3. Every binary separating family has $K \ge \lceil \log_2 |\mathcal{P}| \rceil$, so logarithmic length is optimal up to a constant factor (labels with more than two outcomes can beat the binary bound). For ECM the conservative binary success bit collapses the construction-denominator and final projective-Z paths into one coordinate; analogous collapses define the bit for the $p \pm 1$ methods.

Proposition 32.4 (the label criterion)**.** *Let p and q be distinct odd primes, $N = pq$, and let the deterministic computation on N take the gcds of the denominator, of a_{24} and of $a_{24} - 1$, of the stage-1 Z-coordinate, and run a stage 2 that tests exactly the relations $[v]Q = O$ for $1 \le v \le B_2$ through the x-coordinate atoms described in Section 34: identity atoms $[v]Q = O$, taken first, and collision atoms $x([tm]Q) = x([r]Q)$, $1 \le r < m$, $1 \le t$, formed only from points that are the identity modulo neither prime. In the projective form $X_1Z_2 - X_2Z_1$ a point with $Z \equiv 0$ modulo a prime is the identity there whatever its X – the ladder returns the identity as $(X : 0)$, and as $(0 : 0)$ when it is reached as $[j]Q = O$ with $x([j-1]Q) = x(Q) = \pm 1$, i.e. from a point of order 4 with $[2]Q = (0,0)$ – so the identity atoms detect every such point: one that is the identity modulo one prime only is a proper factor, and one that is the identity modulo both is excluded from all subsequent collision atoms. For the remaining points, whose Z is a unit modulo both primes, a collision atom vanishes modulo a prime exactly when the affine x-coordinates agree there, i.e. when $[tm]Q = \pm[r]Q$, i.e. when $[tm + r]Q = O$ or $[tm - r]Q = O$ modulo that prime, since on a Montgomery curve the x-coordinate determines a point up to sign. Then the curve factors N if and only if $\lambda_\sigma(p) \ne \lambda_\sigma(q)$; moreover, if each identity atom $[v]Q = O$ is assigned the key v and each collision atom $x([tm]Q) = x([r]Q)$ the key $tm + r$, an implementation scanning the atoms in nondecreasing key order may stop at the first vanishing two-sided atom.*

Proof. If the negative labels differ, or if exactly one of the two labels is negative, one of the three construction gcds is proper. If both labels are non-negative and differ, let D_p, D_q be the actual orders of the two stage-1 points. Since the labels differ, at least one of D_p, D_q is at most B_2; let $a \le B_2$ be the smaller exposed order and $e > a$ the other actual order (either both are at most B_2 and unequal, or the label on the e-side is 0 and $e > B_2$). Write $a = tm + r$ with

$m = \lfloor\sqrt{B_2}\rfloor + 1$ and $0 \le r < m$. The atom at key a – the baby identity $[a]Q = O$ if $t = 0$, the giant identity $[tm]Q = O$ if $r = 0$, or the collision $x([tm]Q) = x([r]Q)$ – vanishes modulo the a-side; on the other side it tests only the relation indices a and $tm - r < a$, neither a multiple of $e > a$, so it does not vanish: the atom is one-sided. Every atom of key smaller than a tests only relation indices smaller than a, hence vanishes on neither side, so the first vanishing atom in key order is one-sided and the scan may stop at the first vanishing two-sided atom. Conversely, equal labels yield only two-sided outcomes: the same construction degeneracy occurs on both sides; no relation occurs when both orders exceed B_2; or, when $d_p = d_q$, each tested relation has the same truth value on the two sides ($[v]Q = O$ holds on both exactly when $d_p \mid v$; every vanishing identity atom is then two-sided and its point excluded, and every remaining point has a unit Z on both sides, so each collision atom vanishes on both sides or on neither). □

Distinct label vectors $(\lambda_{\sigma_i}(p))_i$ over $\mathcal{P}$ therefore certify that the list factors every product of distinct primes of $\mathcal{P}$. The collapsed bit $[\lambda \neq 0]$ of Proposition 32.2 is sufficient but discards most of the information. The stopping clause is for a scan in nondecreasing key order; a preparatory scan of the identity atoms in a different order (Section 34) must not stop at a two-sided identity, and must exclude its point from the collision atoms.

33. How long must the list be?

33.1. **The random-signature law.** If independent random curves succeed with probability θ on each prime, one binary coordinate fails to distinguish a fixed pair with probability $R(\theta) = \theta^2 + (1-\theta)^2$, so the expected number of unresolved pairs after K curves is $\binom{n}{2}R(\theta)^K$ and the separation threshold is $K \approx 2\ln n/(-\ln R(\theta))$. Since $R(\theta) \ge 1/2$ with equality at $\theta = 1/2$, a binary coordinate removes the largest fraction of unresolved pairs when its success rate is one half – for a *separating* family the per-member success rate should be tuned to $1/2$, not maximised, and near-fair signatures separate n primes in about $2\log_2 n$ members. For a label with distribution (π_s) the collision probability is $R_{\text{label}} = \sum_s \pi_s^2$, and a larger alphabet can separate faster without changing the group operations. These are heuristics, checked below.

Conjecture 33.1 (E, explicit ECM separation)**.** *For fixed $u > 1$ and $C > 1$ put $B_1 = x^{1/u}$, $B_2 = B_1^2$. There is $C_{u,C}$ such that the first $C_{u,C}\log x$ Suyama parameters, run with stage 1 and the exact stage 2, have distinct exposure-label signatures on all primes in $[x, Cx]$ for all sufficiently large x.*

If true, the list factors every $N = pq$ with distinct primes and $q/p \le C$ deterministically in $N^{1/(2u)+o(1)}$ ring operations: choose $x = \sqrt{N/C}$, so both factors lie in $[x, Cx]$; stage 1 costs $B_1^{1+o(1)}$ and a stage 2 that evaluates the product of the baby polynomial at all giants by one product tree and one quasi-linear multipoint evaluation costs $B_2^{1/2+o(1)} = B_1^{1+o(1)}$. At $u = 3$ this is $N^{1/6+o(1)}$. Taken for every fixed u, the conjecture gives, in this bounded-ratio setting, a deterministic N^{ε} algorithm for every fixed $\varepsilon > 0$ (one algorithm per ε), so it is deliberately strong; finite tests can expose an exceptional-prime tail but cannot establish it. The conjecture concerns the unbounded list; the implementation of Section 34 caps its list and evaluates stage 2 in fixed blocks, and neither restriction belongs to the asymptotic statement.

33.2. **Randomised lists.** Conjecture 33.1 asks for an *explicit* list. For a random list, separation follows from bounds on the exposure probabilities alone. Let μ be the distribution that draws a, x_0, y_0 uniformly from $[1, M]$ with $M \ge x^3$ and forms the curve $y^2 = x^3 + ax + b$, $b := y_0^2 - x_0^3 - ax_0$, with the point $P = (x_0, y_0)$ (Lenstra's ensemble [50]); its labels are defined as in Section 32 with the singular curves as the degenerate state. For a prime p write θ_p for the probability that a curve drawn from μ has a non-zero label at p.

Proposition 33.2 (randomised separation)**.** *Fix $u > 1$ and a constant $\theta \in (0, 1/2]$, let $B_1 = x^{1/u}$, $B_2 = B_1^2$, and suppose that every prime $p \in [x, 2x)$ satisfies $\theta \le \theta_p \le 1 - \theta$. Then for $x \ge x_0(u, \theta)$, $K := \lceil 3 \log x/(\theta(1-\theta)) \rceil$ independent draws from μ have pairwise distinct exposure-label vectors on all primes of $[x, 2x)$ with probability at least $1 - 1/x$.*

Proof. Fix distinct primes $p, q \in [x, 2x)$. The label at p depends only on $(a, x_0, y_0) \bmod p$ and the label at q only on the reduction modulo q; since $M \ge x^3 \ge pq \cdot x/4$, the joint distribution of the two reductions is within total variation $O(1/x)$ of the product of uniform distributions (Chinese remainder theorem), so the two labels are independent up to that error. Write $\pi_p(s)$ for the probability of the label s at p. Then

$$\Pr[\lambda_p = \lambda_q] \;\le\; (1-\theta_p)(1-\theta_q) + \pi_p(1)\pi_q(1) + \sum_{s \ge 2} \pi_p(s)\pi_q(s) + \Pr[\text{both degenerate}] + O(1/x).$$

The degenerate term is $O(1/x^2)$. If the label at p is $s \ge 2$ then, for every prime $\ell \mid s$, $\ell^{v_\ell(L)+v_\ell(s)}$ divides the order of P and hence $\#E(\mathbb{F}_p)$, so $m_s := s \prod_{\ell \mid s} \ell^{v_\ell(L)}$ divides $\#E(\mathbb{F}_p)$, and $m_s > B_1$ because $\ell^{v_\ell(L)+1} > B_1$ by the definition of L. Let $\mathcal{S}_m(p) := \{n : |n - (p+1)| \le 2\sqrt{p},\ m \mid n\}$, so that $|\mathcal{S}_m(p)| \le 4\sqrt{p}/m + 1$. We use the following estimate, which follows from the ingredients of Lenstra's Proposition (1.16) [50] – Deuring's theorem, which expresses the number of pairs (a, b) with a given order through a Kronecker class number, and the class-number bound $H(\Delta) \ll |\Delta|^{1/2}(\log|\Delta|)(\log\log|\Delta|)^2$ – applied to every order in the Hasse interval (Lenstra states the proposition for $|n-(p+1)| < \sqrt{p}$, a restriction his lower bound needs and the upper bound does not), and transferred from uniformly random curves to the curve-with-point ensemble μ, whose weighting by the chosen point changes each probability by a factor $1 + O(p^{-1/2})$ and whose finite box adds a discrepancy $O(p/M)$: the probability under μ that m divides $\#E(\mathbb{F}_p)$ is at most $C(\log p)(\log\log p)^2(1/m + p^{-1/2})$. Hence $\pi_p(s) \le C(\log p)(\log\log p)^2(B_1^{-1} + p^{-1/2})$ uniformly in $s \ge 2$, and $\sum_{s \ge 2} \pi_p(s)\pi_q(s) \le \max_{s \ge 2} \pi_p(s) = o(1)$. Since $\pi_p(1) \le \theta_p$, the remaining terms are at most $(1-\theta_p)(1-\theta_q) + \theta_p\theta_q = 1 - \theta_p - \theta_q + 2\theta_p\theta_q$, a bilinear function whose maximum over $\theta_p, \theta_q \in [\theta, 1-\theta]$ is $1 - 2\theta(1-\theta)$. So one draw fails to separate p from q with probability at most $1 - \theta(1-\theta)$ for $x \ge x_0(u, \theta)$, chosen so that the $o(1)$ terms total at most $\theta(1-\theta)$; K independent draws fail with probability at most $\exp(-K\theta(1-\theta)) \le x^{-3}$, and a union bound over the fewer than x^2 pairs gives the claim. □

The hypothesis is two-sided: a lower bound on the exposure probability is the hypothesis on smooth numbers in the Hasse interval under which the running time of ECM is analysed [50], and an upper bound could come, for example, from a positive proportion of point orders with a prime factor above B_2 (other residual orders exceeding B_2 are possible too), which is open for the same short-interval reasons; heuristically $\theta_p \approx 0.45$ at $u = 3$ for this ensemble [3], and the measured Suyama rates are 0.69–0.81 (Table 12). Conditionally on the hypothesis, the resulting non-uniform curve-list advice has $O(\log x)$ curves and $O(\log x \log M)$ bits – $O(\log^2 x)$ bits for $M = x^{O(1)}$; what Conjecture 33.1 adds is explicitness (and the passage to the Suyama family, for which the same argument needs the analogue of the class-number bound).

33.3. **Full-population computations.** For every prime of the dyadic intervals $[x, 2x)$, $x = 2^{14}, 2^{16}, 2^{18}, 2^{20}, 2^{22}$ ($n = 1612, 5709, 20390, 73586, 268216$ primes), the labels of the Suyama curves $\sigma = 6, 7, \ldots$ were computed exactly at $B_1 = \mathrm{round}(x^{1/u})$, $B_2 = \mathrm{round}(x^{2/u})$ by a vectorised Montgomery ladder. The computation refines the partition of the primes by label prefix curve by curve, and computes a later curve's label only for the primes whose class in the exact partition or in the binary partition is not yet a singleton; since classes only refine, this determines the coverage and separating lengths exactly without computing the whole label matrix. The label routine is checked in the accompanying test suite against scalar point orders and, end to

end, against the algorithm (one curve factors pq iff the labels differ, on every pair of consecutive primes of a small range).

u	x	n	B_1, B_2	exposed rate (curve 1)	K_{cov}	$K_{\mathrm{sep}}^{\mathrm{label}}$	K_{sep} binary
3	2^{14}	1612	$25,645$	0.806	5	6	79
3	2^{16}	5709	$40,1625$	0.769	7	7	51
3	2^{18}	20390	$64,4096$	0.746	10	10	47
3	2^{20}	73586	$102,10321$	0.715	12	11	46
3	2^{22}	268216	$161,26008$	0.691	13	12	> 40
4	2^{14}	1612	$11,128$	0.407	20	19	27
4	2^{16}	5709	$16,256$	0.324	33	31	34
4	2^{18}	20390	$23,512$	0.311	35	32	34
4	2^{20}	73586	$32,1024$	0.291	41	36	46
4	2^{22}	268216	$45,2048$	0.253	53	53	55

TABLE 12. Covering length (every prime exposed by some curve), label-separating length (all label vectors distinct) and the separating length of the binary projection $[\lambda \neq 0]$, on every prime of $[x, 2x)$. At $u = 3$, $x = 2^{22}$ the binary projection had not separated after the 40 curves computed (18 pairs remained unresolved).

The exact labels separate in 6–12 curves at $u = 3$ – $6, 7, 10, 11, 12$ at $x = 2^{14}, 2^{16}, 2^{18}, 2^{20}, 2^{22}$, i.e. increments of $1, 3, 1, 1$ across successive quadruplings of x – consistent with slow, at most logarithmic, growth. The binary projection of the same predicate needs 46–79 on the four smaller intervals, because its success rate 0.69–0.81 is far from the optimal $1/2$, as the design rule predicts. A coarser bit does better: call the *one-large-prime bit* of a curve at p the event that the construction denominator vanishes, the stage-1 point is the identity, or the residual order is a prime in $(B_1, B_2]$ – the classical stage-2 success condition, which omits the singular states and the composite residual orders; it separates the four smaller populations in $24, 32, 39, 37$ curves. Hence *for* $(B_1, B_2) = (64, 4096)$ *the first ten Suyama curves are a finite certificate for every product of distinct primes in* $[2^{18}, 2^{19})$*, for* $(102, 10321)$ *the first eleven certify* $[2^{20}, 2^{21})$*, and for* $(161, 26008)$ *the first twelve certify* $[2^{22}, 2^{23})$ – computer-verified separating lists whose certificate is the parameter pair and the list of curves, verified by recomputing the labels, which the accompanying code does in minutes; the archived record is the class counts after each curve. At 2^{22} the uncovered fraction after k curves is $0.309, 0.097, 0.030, 0.010, 0.0033, \ldots$, close to 0.31^k, and the last pair is separated by the twelfth curve. (With parameters derived from N the certificates do not apply literally.) At $u = 4$ the exact labels separate every pair on all five intervals; the lengths $31, 32, 36, 53$ at $x = 2^{16}, \ldots, 2^{22}$ have increments $+1, +4, +17$, the last far larger than the earlier ones.

The separation tail is structured. For the six one-large-prime runs on the three smaller intervals (stage 1 alone and with the stage-2 continuation), the pairs still unresolved at the last recorded snapshot before separation number 311 in all, and $p \equiv q \pmod 3$ holds for 195 of them (0.63), compared with 0.50 for random pairs of the same populations. This is a finite verified enrichment; its explanation through the residue dependence of curve orders on $p \bmod 3$ is heuristic. *Plain* Montgomery curves – $A = 7, 8, \ldots$ with starting x-coordinate 3, without Suyama's forced 3-torsion – have one-large-prime success rate near $1/2$ at $u = 3$ and separate the three smaller populations in $22, 26, 30$ curves by that bit, compared with Suyama's $24, 32, 39$ and the birthday thresholds $2 \log_2 n = 21.3, 24.9, 28.6$.

34. The algorithm

The implementation tests N for a perfect square, derives $x = \sqrt{N/C}$, $B_1 = \mathrm{round}(x^{1/u})$, $B_2 = \mathrm{round}(x^{2/u})$, and runs $\sigma = 6, 7, \ldots$, capped at 400 curves. For each curve, the implementation takes the construction gcd and the singularity gcd $\gcd(a_{24}(a_{24}-1), N)$, backtracking to $\gcd(a_{24}, N)$ and $\gcd(a_{24}-1, N)$ when that gcd equals N; runs stage 1 and takes the gcd of its projective Z-coordinate; and runs a stage 2 over $\mathbb{Z}/N$ with $m = \lfloor\sqrt{B_2}\rfloor + 1$, $T = \lfloor B_2/m \rfloor$, $R = B_2 - Tm$: baby points jQ, $1 \le j < m$, giant points $i(mQ)$, $1 \le i \le T$, preparatory identity gcds (a proper gcd is returned at once; a point that is the identity modulo both primes, whose gcd is N and carries no factor, is removed from the baby and giant lists and the search continued), batch inversion, $F(t) = \prod_j (t - x(jQ))$ by a product tree evaluated at the giants $i < T$, the partial product over $j \le R$ at giant T, the gcd of the product, and, when backtracking is required, gcds of the $O(\sqrt{B_2})$ row products in increasing giant order followed by at most $O(\sqrt{B_2})$ individual atoms of the first non-trivial row in the nondecreasing key order of Proposition 32.4 (babies increasing within the row) – $O(\sqrt{B_2})$ gcds, not a scan of B_2 atoms – stopping at the first vanishing two-sided atom. The tested values are exactly $[1, B_2]$, so the curve factors N iff the labels of Proposition 32.4 differ. Per curve the ladder work is $O(B_1)$ group operations. The evaluation of F at the giants is done in fixed blocks of 4096 points, each block evaluated independently, to bound memory; this is not the single quasi-linear multipoint evaluation of the complexity statement after Conjecture 33.1, and no asymptotic claim is made for the blocked form.

Measurements. By *counted multiplications* we mean the number of modular multiplications performed in the Montgomery ladders and differential additions, the products of projective Z-coordinates, the batch inversions and the row products; the coefficient arithmetic inside the product tree and the multipoint evaluation is not counted. With the explicit parameters $(64, 4096)$, on 500 random prime pairs from $[2^{18}, 2^{19})$ (unordered, distinct, from a seeded generator) plus the 116 distinct pairs of the one-large-prime separation tail of that interval, all 616 were factored (maximum 3 curves, mean 1.08, counts 565/50/1 at one/two/three curves; 145 by stage 1, 471 by stage 2; the algorithm succeeded no later than the one-large-prime separation index – the first curve whose one-large-prime bits differ at p and q – on every pair, and strictly earlier on 54.7%). On 20 balanced semiprimes per size ($q/p < \sqrt{2}$, from a seeded generator) at $32, 40, 48, 56, 64$ bits with $u = 3$, $C = 2$ and N-derived parameters, the mean curve count is 1.0–1.2, the mean counted multiplications per modulus are $1104, 2715, 8920, 22\,725, 48\,358$, and the fitted exponent of the counted multiplications against the bit size is 0.175 against the prediction $1/(2u) = 0.167$ up to logarithmic factors, with a curve-count exponent of 0.003. Scaling, on single instances with wall-clock times and peak resident memory: blocking the multipoint evaluation cut a 128-bit $u = 3$ run from 179 s and 6.46 GiB to 96 s and 3.01 GiB; over the 120-, 124-, 128- and 136-bit instances the peak memory fits the empirical line $1.46\,\mathrm{KiB} \cdot B_1 + 13$ MiB; fixed $u = 3$ reached 136 bits in 203 s with 7.78 GiB, while larger u trades memory for curves ($u = 4$: 144 bits in 129 s and 405 MiB with 3 curves, 160 bits in 81 s and 1.44 GiB with 1 curve; $u = 5$: 180 bits in 671 s and 422 MiB with 10 curves). A greedy multi-u schedule – choosing at each step, among the curves $\sigma = 6, \ldots, 17$ at each of $u \in \{2.5, 3, 3.5, 4, 4.5\}$, the one resolving the most pairs per unit of B_1 – was slightly worse than the best separating fixed-u prefix from the same candidates on the two populations tested (152 against 150; 324 against 264 in the work proxy $\sum B_1$): cheap high-u coordinates leave an expensive cleanup tail.

35. What the route can and cannot give

Write $L_N[s, c] := \exp\big((c + o(1))(\log N)^s (\log\log N)^{1-s}\big)$. Each curve's exposure probability is modelled heuristically by the semismoothness [3] of a group or point order of size $N^{1/2+o(1)}$, so,

under the random-signature and semismoothness heuristics extrapolated uniformly as u grows, the optimised fixed-list model is $L_N[1/2,1]$ – the classical ECM heuristic, here as the cost of a fixed list – against the number field sieve's $L_N[1/3,(64/9)^{1/3}]$ [64]: in leading L-formulas, $2^{65.9}$ against $2^{63.9}$ operations at 512 bits, $2^{98.5}$ against $2^{86.8}$ at 1024, $2^{146.4}$ against $2^{116.9}$ at 2048 – formal values of the leading formulas, not operation counts of implementations. Exact labels, torsion families, better chains and batching change constants; the route's content is determinism and the finite certificates, not speed.

Proposition 35.1 (non-uniform derandomisation)**.** *Let $U_n = L_{2^n}[1/2,1]$ uniformly bound the expected running time – measured in bit operations, each random bit read costing one operation – of the Lenstra–Pomerance algorithm [54] on n-bit inputs. For every n there is an advice string w_n of length $O(nU_n)$ such that a deterministic algorithm with access to w_n factors every n-bit integer in time $O(nU_n)$.*

Proof. Run the algorithm with a fixed random string truncated after $4U_n$ steps; by Markov it succeeds with probability $\geq 3/4$ on every input. With $n+1$ independent strings the failure probability on a fixed input is $\leq 4^{-(n+1)}$, and the union bound over the $< 2^n$ inputs shows that some choice of strings succeeds on all of them. Each truncated run consumes $O(U_n)$ random bits, so the concatenated advice has length $O(nU_n)$. □

This is Adleman's argument [1] with subexponential advice. A uniform deterministic subexponential algorithm would follow from an explicit construction of such advice; a smoothness separating family is one candidate shape for it, and Conjecture 33.1 is the fixed-u version.

Proposition 35.2 (Miller's descent)**.** *Let p,q be distinct odd primes, $N=pq$, $\gcd(\alpha,N)=1$, $\operatorname{ord}_p(\alpha)=2^{j_p}u_p$ and $\operatorname{ord}_q(\alpha)=2^{j_q}u_q$ with u_p,u_q odd, and let $E=2^s m$ (m odd) be a common multiple of the two orders, as delivered by a two-sided $p-1$ collision $\alpha^E\equiv 1 \pmod N$. Testing $\gcd(x_j-1,N)$ along the binary chain $x_j=\alpha^{2^j m}$, $0\leq j\leq s$, yields a proper factor iff $j_p\neq j_q$.*

Proof. Since both orders divide E, $u_p,u_q \mid m$ and $j_p,j_q\leq s$, so $x_j\equiv 1 \pmod p$ first at $j=j_p$ and $\pmod q$ first at $j=j_q$. If $j_p<j_q$ then $\gcd(x_{j_p}-1,N)=p$, and symmetrically; if $j_p=j_q>0$ then x_{j_p-1} has order 2 modulo both odd primes, hence is -1 modulo both, and no gcd in the chain is proper; if $j_p=j_q=0$ there is no 2-adic descent. □

This is the criterion for Miller's binary chain [59] only: descent by an odd prime dividing one order and not the other can recover further cases when E can be factored.

A positive-density success theorem. The asymptotic running-time conclusions above for the explicit fixed-list smooth-order route are heuristic or conditional. We give one unconditional positive-density statement about the smooth-order route. It is an elementary corollary of two classical theorems on shifted primes, and we record it as the rigorous reference point of the route: it concerns the success set of a deterministic *partial* factoring algorithm – one allowed to fail on a complementary positive proportion – and is not an average running-time bound for an algorithm that factors every input. Let $P^+(n)$ denote the largest prime factor of n. Friedlander [26] proved that for every $\theta > 1/(2\sqrt{e}) = 0.30326\ldots$ there is $c_1(\theta)>0$ with $\#\{p\leq x : P^+(p-1)\leq x^\theta\}\geq c_1 x/\log x$ for all large x – a positive proportion of the primes; the record exponents 0.2961 [4] and 0.2844 [51] are stated as infinitude results (infinitely many primes p with $P^+(p-1)\leq p^\theta$), not as positive proportions. Fouvry [25] proved that there is a fixed exponent $\alpha>2/3$ – one may take $\alpha=0.6687$ in the published numerical form – and $c_2>0$ with $\#\{q\leq x : P^+(q-1)\geq q^\alpha\}\geq c_2 x/\log x$. The algorithm $\mathcal{A}_\theta$ is Pollard's $p-1$ method [68] with base 2: on input N put $B:=\lceil N^{\theta/2}\rceil$, $E:=\prod_{\ell\leq B,\ \ell \text{ prime}} \ell^{\lfloor \log N/\log \ell\rfloor}$ and $g:=\gcd(2^E-1 \bmod N,\ N)$, and output g if $1<g<N$. It is deterministic. Since $\log_2 E\leq \pi(B)\log_2 N$, binary exponentiation (prime power

by prime power, without materialising E) costs at most $2\pi(B)\log_2 N + O(1)$ multiplications modulo N; with $\pi(B) \ll B/\log B$ and $\log B = (\theta/2)\log N + O(1)$ this is $O_\theta(B) = O_\theta(N^{\theta/2})$. Prime generation and the final gcd add only factors polynomial in $\log N$ to the bit complexity.

Proposition 35.3 (positive-density success of the $p-1$ method)**.** *Fix $\theta \in (1/(2\sqrt{e}), 1/2)$ and $\varepsilon \in (0, 1/4)$ with $\theta(1-\varepsilon) > 1/(2\sqrt{e})$. There are $c = c(\theta,\varepsilon) > 0$ and x_0 such that for every $x \ge x_0$, at least $c\,\pi(x)^2$ of the ordered pairs (p,q) of distinct primes in $(x^{1-\varepsilon}, x]$ satisfy $\mathcal{A}_\theta(pq) = p$. Hence a positive relative proportion of the semiprimes $N = pq$ with $x^{1-\varepsilon} < p, q \le x$ are factored deterministically in $O_\theta(N^{\theta/2})$ multiplications modulo N. For fixed ε the admissible exponent $\theta/2$ can approach $1/(4\sqrt{e}(1-\varepsilon))$; letting $\varepsilon \downarrow 0$ and $\theta \downarrow 1/(2\sqrt{e})$ jointly, subject to $\theta(1-\varepsilon) > 1/(2\sqrt{e})$, brings it arbitrarily close to $1/(4\sqrt{e}) = 0.151632\ldots$.*

Proof. Put $\theta' := \theta(1-\varepsilon)$ and $S := \{p \in (x^{1-\varepsilon}, x] : P^+(p-1) \le x^{\theta'}\}$; by Friedlander's theorem at θ', $|S| \ge c_1(\theta')x/\log x - \pi(x^{1-\varepsilon}) \ge \frac{1}{2}c_1 x/\log x$ for large x. Let $\Omega := \{q : \mathrm{ord}_q(2) \le x^{1-\alpha}\}$; a prime with $\mathrm{ord}_q(2) = d$ divides $2^d - 1$, which has fewer than d prime factors, so $|\Omega| \le \sum_{d \le x^{1-\alpha}} d \le x^{2-2\alpha} = x^{0.6626}$. Let $G := \{q \in (x^{1-\varepsilon}, x] : P^+(q-1) \ge q^\alpha\} \setminus \Omega$; by Fouvry's theorem $|G| \ge \frac{1}{2}c_2 x/\log x$ for large x. Take $p \in S$, $q \in G$, $p \ne q$, and $N := pq \in (x^{2-2\varepsilon}, x^2]$. (i) $B \ge N^{\theta/2} > x^{\theta'} \ge P^+(p-1)$, and every prime power $\ell^v \,\|\, p-1$ has $\ell^v < N$, so $v \le \lfloor \log N/\log \ell \rfloor$; hence $p-1 \mid E$ and $p \mid 2^E - 1$. (ii) If $q \mid 2^E - 1$ then $\mathrm{ord}_q(2) \mid E$ is B-smooth. Since $B \le x^\theta + 1 < x^{\alpha(1-\varepsilon)} < q^\alpha \le P^+(q-1)$ for large x (as $\alpha(1-\varepsilon) > 3\alpha/4 > 1/2 > \theta$), the prime $P^+(q-1)$ does not divide $\mathrm{ord}_q(2)$, and $\mathrm{ord}_q(2) \mid q-1$ gives $\mathrm{ord}_q(2) \le (q-1)/P^+(q-1) < q^{1-\alpha} \le x^{1-\alpha}$, i.e. $q \in \Omega$, a contradiction. So $g = \gcd(2^E - 1, N) = p$. (iii) The pairs number at least $|S||G| - |S \cap G| \ge \frac{1}{4}c_1 c_2 (x/\log x)^2 - x \ge c\,\pi(x)^2$ for large x, with $c := c_1 c_2/7$, by $\pi(x) \le 1.26\,x/\log x$ [74]. Each semiprime pq arises from at most two ordered pairs, so the semiprimes factored number at least $c\,\pi(x)^2/2$, a positive proportion of the fewer than $\pi(x)^2/2$ semiprimes of the family. □

Remarks. (a) On $S \times G$ neither the two-sided outcome $g = N$ nor the failure $g = 1$ occurs; on the whole population both do. (b) For independent primes near x the smoothness heuristic predicts that $p-1$ is x^θ-smooth with probability $\varrho = \rho(1/\theta)$ (Dickman's ρ); if in addition the exceptional event $\mathrm{ord}_p(2) \mid E$ with $p-1$ not B-smooth has density $o(1)$, the idealised one-sided success rate is $2\varrho(1-\varrho)$. At $\theta = 0.31$, $\rho(3.2258\ldots) = 0.02997$ and $2\varrho(1-\varrho) = 0.0582$ – a Dickman proxy, not an established asymptotic; the lower-bound set S of the proof has the smaller parameter $\theta' = \theta(1-\varepsilon)$ and Dickman density $\rho(1/\theta')$. We ran $\mathcal{A}_{0.31}$ on 2000 balanced semiprimes ($q/p < \sqrt{2}$, from a seeded generator) at each of $40, 48, 56, 64$ bits, with $B = \lceil N^{0.155} \rceil$ between 67 and 967: it factored $204, 178, 165, 152$ of them ($0.102, 0.089, 0.083, 0.076$, binomial standard errors below 0.007), returned $g = N$ for $8, 8, 6, 7$, and failed on the rest – decreasing over these four sizes and above the proxy, consistent with a finite-size excess of smooth shifted primes; the data do not establish convergence. The order anomaly of step (ii) – a factor whose shifted prime is not B-smooth but whose order of 2 divides E – occurred for $2, 2, 0, 0$ of the 2000 moduli. (c) With the stage 2 of Section 34 ($B_2 = B^2$, cost still $B^{1+o(1)}$), a (B, B^2)-semismooth $p-1$ is a sufficient exposure condition on the p-side, not a necessary one ($\mathrm{ord}_p(2)$ may be a proper divisor of $p-1$); a one-sided theorem again needs the other side excluded, which the Fouvry set provides by the same order argument when $B^2 < P^+(q-1)$, i.e. for $2\theta < \alpha(1-\varepsilon)$. In the same samples exactly one of $p-1, q-1$ is (B, B^2)-semismooth for $0.496, 0.482, 0.504, 0.483$ of the moduli (a measurement, not an asymptotic statement); a positive-proportion theorem for $p-1 = (x^\theta\text{-smooth}) \times (\text{prime} \le x^{2\theta})$ at some $\theta < 1/(2\sqrt{e})$ would lower the exponent of Proposition 35.3 accordingly, and we have not found one: the shifted-prime results available [26, 25, 4, 51] concern smoothness or a large prime factor alone. (d) Harvey's $N^{1/5}$ [31] is a worst-case bound valid for every N; given any slack $\delta > 0$, choosing first the balance parameter $\varepsilon > 0$

$\Lambda_d(P_{\min})$ 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