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.

(Proposition 20.1); the Beatty chains, forcing $D_{\max} \gg \sqrt{r}$ on the full shell for $r \lesssim N^{1/4}$; the near-chains (Proposition 20.2); the two-progression normal form and its integrality conditions (Proposition 20.3, Lemma 20.4); the modulus-free lower bound $D^*_\theta(r) \geq (c_\theta - o(1))r^{1/3}$ with the sharp constant of the symmetric mechanism (Theorems 20.8, 20.11) and the transfer between the exact-start and modulus-free statistics (Lemma 20.9); the class count $n \leq 2^{\omega(q)}$, the long-period bound and the envelope $7\,r^{1/3}$ for every drift-free family with $\Delta_d \neq 0$ (Lemmas 20.14, 20.15, Theorem 20.16); the planar cap (Proposition 21.1); the resonant clusters $\gg N^{1/12}$ at $r = N^{1/3}$ for the full shell at every N (Theorems 21.2, 21.4) and for the squarefree shell for almost all N (Theorem 21.3); the sliding-window bound and its consequences (Theorem 21.5, Corollary 21.6); the planar two-progression envelope and the thin resonant hierarchy (Theorem 21.10, Corollary 21.11); the unconditional upper bounds $6N^{2/9}$ at $r = N^{1/3}$ and $2.1\,r^{2/3}$ for the modulus-free statistic (Theorems 21.13, 21.14); the near-minimal additive energy (Proposition 21.15) and the energy form of Lemma 4.3; and the ceilings of Corollaries 21.7, 21.8 on what Lemma 4.3 can certify through whole shells. For the balanced restriction: the rays (Lemma 19.1), the equal-product pairs (Lemma 19.2) and the half-offset families (Lemma 19.3), which give $D_{\max} \geq rN^{-1/4}/15 - 2$ for every family retaining the constructed cells, in particular for the primitive balanced family.

Conditional. Under Conjecture 19.4, Proposition 19.5 gives $|B| + |G| \gg_C N^{5/28-o(1)}$; under Conjecture 19.6, Corollary 19.7 gives $N^{2/11-o(1)}$; under the envelopes (S″) below the crossing and (P′) beyond it, Theorem 4.4 gives $N^{2/11-o(1)}$, which by Corollary 21.7 is also the most the whole-shell certificate can give; under (T) and (T_P), Theorem 4.4 gives $N^{1/5-\delta}$ for every $\delta > 0$. The application of Lemma 19.3 to the unique-product family is conditional on the constructed cells being its representatives. The extremality conjectures (S‴), (P‴) and the first-order computations – offset resonance, the general-W profile, the cost side of the refined-prime programme – are marked as such where they occur.

Computed. The censuses of Section 23: the modulus-free sweeps and the drift-free family census, the symmetric family, the planar and resonant censuses to 96 bits, the energy and non-drift-free computations, the direct cover search and the balanced censuses, each with its exactness status and its controls.

Open. The upper envelope of $D_{\max}$ – between the proved exponent $2/3$ and the conjectured $1/4$ (as powers of the shell size) at the top of the range, and between $2/3$ and $1/3$ for the modulus-free statistic; whether a single drift-free family carries the maximum up to $o(r^{1/3})$; the excision estimate that Conjecture 19.6 needs (an $O_C(r/M)$ incidence bound for the cells in high-window half-offset configurations, against the provable $O(r^{4/3}/M^2)$); the representative property of the half-offset cells in the unique-product family; and the positive-proportion squarefree problem in short intervals that separates Theorem 21.2 from its squarefree analogue for every individual N. Nothing in this part bounds the cost of factoring: every floor is a statement about the explicit-difference representation model, and inside that model the results leave open representations at the $N^{2/11+o(1)}$ scale, none of which is constructed here.

Part 4. Factoring $N = pq$ from N alone when $\gcd(p-1, q-1)$ is large

Summary. Let $N = pq$ with primes $p < q$ be balanced, $\sqrt{N/C} \leq p < \sqrt{N}$ for a fixed $C > 1$, and let $g := \gcd(p-1, q-1)$. For any unit α with $\alpha^{N-1} \not\equiv 1 \pmod N$, a babystep–giantstep search on $\beta := \alpha^{N-1}$ factors N deterministically in $O(N^{1/4}/\sqrt{g})(\log N)^{O(1)}$ bit operations, using nothing but N. Some $\alpha \leq (\log N)^4$ qualifies unless $g > (p-1)^{3/4}/(\log N)^3$, by a count of smooth numbers inside the subgroup of Fermat liars; in the remaining class Burgess's character-sum bound supplies a base below $N^{1/(8\sqrt{\mathrm{e}})+\varepsilon}$ for every $\varepsilon > 0$. Consequently every balanced semiprime with $g \geq N^{5/24}/(2\sqrt{C}(\log N)^3)$ is

factored from N alone with exponent below $1/5$; writing $g = N^\gamma$, the exponent $1/4 - \gamma/2$ is below $1/5$ for every $\gamma > 1/10$. Composing the McKee–Pinch progression search, made deterministic, with Pollard–Strassen on $N-1$ and Harvey–Hittmeir's order selection gives a curve $E(\gamma)$ that is below $1/5$ for every $\gamma > 1/20$. The exponent $1/4 - \gamma/2$ from N alone is that of McKee and Pinch's Pollard-rho variant with iteration $x \mapsto x^{N-1} + 3$, an expected-time attack restated by Hinek; the present argument is its deterministic form – a babystep–giantstep search with the base chosen deterministically – and needs no knowledge of g.

25. Introduction and context

Throughout, $N = pq$ with distinct primes $p < q$, and for a fixed $C > 1$ the smaller factor lies in the balance range $J_C := [\sqrt{N/C}, \sqrt{N}]$, so that $p, q = \Theta_C(N^{1/2})$; "N large" means large in terms of C. Write

$$g := \gcd(p-1, q-1), \qquad k := \frac{p-1}{g}, \qquad l := \frac{q-1}{g}, \qquad \gcd(k, l) = 1.$$

Moduli with a large g were proposed by Wiener [81] as a defence against his small-exponent attack, and are studied under the name "common prime RSA" by Hinek [37, 38]. Attacks from N alone are part of that literature: with $g = N^\gamma$, McKee and Pinch [58], as restated in [38, Attack 6.1], factor N in $O(N^{1/4-\gamma/2})$ expected operations by a Pollard-rho variant whose iteration $x \mapsto x^{N-1} + 3$ takes at most $(p-1)/g$ values modulo p; given g, their babystep–giantstep search costs $O(N^{1/4-\gamma})$ expected [38, Theorem 6.4], and for known $g \geq N^{1/4}$ the congruence $(N-1)/(2g) \equiv a + b \pmod g$ factors N in polynomial time [38, Theorem 6.3]; g itself is sought by factoring $(N-1)/2$ [38, §6.3.4]. The small-exponent attacks [37] use the public exponent. Here only N is used, g is not assumed known, and the search is deterministic, so that the exponent $1/4 - \gamma/2$ becomes a proven worst-case bound; Section 28 then combines the progression search behind McKee and Pinch's known-g exponent with a deterministic recovery of g from $N-1$ into the curve $E(\gamma)$ of Proposition 28.2. The starting point is elementary: since $N - 1 = (p-1)q + (q-1) = (q-1)p + (p-1)$,

$$\gcd(N-1, p-1) = \gcd(q-1, p-1) = g, \qquad \gcd(N-1, q-1) = g,$$

so for any unit α the element $\beta := \alpha^{N-1}$ has order dividing $(p-1)/g = k$ modulo p and dividing l modulo q, and these two orders are coprime. A collision search on β therefore has to cover only $\min(k, l) \leq \sqrt{kl} < \sqrt{N}/g$ exponents, a Pollard–Strassen or babystep–giantstep cost of $\tilde{O}(N^{1/4}/\sqrt{g})$. The two questions are how to find a base α that is not a Fermat liar ($\beta \not\equiv 1$) deterministically, and what the resulting bound is worth against the deterministic state of the art, $N^{1/5+o(1)}$ [31, 32].

The search step uses two tools from the deterministic-factoring literature: Hittmeir's lemma that an element of exact order m modulo N has the same order modulo every prime factor iff $\gcd(\beta^{m/r} - 1, N) = 1$ for every prime $r \mid m$ [39, Lemma 2.3], and Harvey's collision algorithm [31, Algorithm 4.1], which finds a collision modulo exactly one prime among n giants and m babies in $O(n \log^3 N + m \log^2 N)$ bit operations under the preconditions that $\mathrm{ord}_N(\alpha) > m$ and no giant equals a baby in $\mathbb{Z}/N\mathbb{Z}$. The base-selection step uses a count of smooth numbers in a subgroup of $\mathbb{F}_p^\times$; the same count drives the order-selection theorem of Harvey and Hittmeir [33] and its balanced-semiprime variant in Section 16. Notation: $\Psi(x, y)$ is the number of y-smooth integers in $[1, x]$, $\pi(y)$ the number of primes up to y, ρ the Dickman function, and $\tilde{O}$ hides factors $(\log N)^{O(1)}$.

26. The collision search

Lemma 26.1 (smooth numbers below p)**.** *For N sufficiently large in terms of C and $y := (\log N)^4$,*

$$\Psi(p-1,y) \;>\; \frac{(p-1)^{3/4}}{(\log N)^3}.$$

Proof. Put $u := \lfloor \log(p-1)/\log y \rfloor$; for N large $u \le \pi(y)$, and the products of u distinct primes $\le y$ are distinct y-smooth integers below p, so $\Psi(p-1,y) \ge \binom{\pi(y)}{u} \ge (\pi(y)/u)^u$. Since $\pi(y) > y/\log y$ for $y \ge 17$ and $u \log y \le \log(p-1)$, $\pi(y)/u > (\log N)^4/\log(p-1) \ge (\log N)^3$, while $u \ge \log(p-1)/(4\log\log N) - 1$; therefore $\Psi(p-1,y) \ge (\log N)^{3u} \ge (p-1)^{3/4}/(\log N)^3$. □

Lemma 26.2 (a large common factor of $p-1$ and $q-1$)**.** *Fix $C > 1$. Let $N = pq$ with distinct primes $p < q$, $p \in J_C$, and N sufficiently large in terms of C. For every unit α with $\alpha^{N-1} \not\equiv 1 \pmod N$, a collision search on $\beta := \alpha^{N-1}$ factors N in $O(\sqrt{\min(k,l)})(\log N)^{O(1)} \le O(N^{1/4}/\sqrt{g})(\log N)^{O(1)}$ bit operations. Moreover some integer $2 \le \alpha \le (\log N)^4$ satisfies $\alpha^{N-1} \not\equiv 1 \pmod N$ unless $g > (p-1)^{3/4}/(\log N)^3$. Consequently every N with*

$$\frac{N^{5/24}}{2\sqrt{C}\,(\log N)^3} \;\le\; g \;\le\; \frac{(p-1)^{3/4}}{(\log N)^3}$$

is factored in $N^{7/48+o(1)}$ bit operations from N alone.

Proof. The image of the power map $x \mapsto x^{N-1}$ on the cyclic group $\mathbb{F}_p^\times$ has order $(p-1)/\gcd(p-1, N-1) = k$, so $\operatorname{ord}_p(\beta) \mid k$; similarly $\operatorname{ord}_q(\beta) \mid l$, and the two component orders are coprime. If exactly one of them is 1, then $\gcd(\beta - 1, N)$ is a proper factor; both are 1 exactly when $\beta \equiv 1 \pmod N$, which is excluded. So assume both exceed 1; being coprime they are distinct. Put $e := \min\{\operatorname{ord}_p \beta, \operatorname{ord}_q \beta\}$: the prime of order e divides $\beta^e - 1$ and the other does not, so $\gcd(\beta^e - 1, N)$ is proper, and $e \le \min(k,l) \le \sqrt{kl} = \sqrt{(p-1)(q-1)}/g < \sqrt{N}/g$.

For $D' = 4, 16, 64, \ldots$ put $H := \sqrt{D'}$ and compare the babies β^i, $0 \le i < H$, with the giants β^{jH}, $1 \le j \le H$; the differences $jH - i$ cover $[1, D']$. An exact equality modulo N gives a positive relation exponent $M = jH - i \le D'$; factoring M by trial division up to $\sqrt{M} \le \sqrt{D'}$, within the budget of this round, and stripping its prime divisors gives the exact order $E = \operatorname{ord}_N(\beta)$, and since the component orders differ, [39, Lemma 2.3] gives a prime $r \mid E$ with $\gcd(\beta^{E/r} - 1, N) > 1$, which is proper because E is exact. If there is no exact equality then $\operatorname{ord}_N(\beta) > D' \ge H$ and the separation preconditions of [31, Algorithm 4.1] hold; once $D' \ge e$ the representation $e = jH - i$ is a collision modulo exactly one prime and Harvey's algorithm returns a factor (directly when the gcd of the evaluated product with N is proper, and by scanning the babies once when it is N, a giant agreeing with one baby modulo p and with another modulo q). The first such D' is below $4e$, and the geometric sum of the costs is $O(\sqrt{e})(\log N)^{O(1)} \le O(N^{1/4}/\sqrt{g})(\log N)^{O(1)}$.

Put $y := (\log N)^4$; for N large, $y < p$, so every $2 \le \alpha \le y$ is a unit. If all of them satisfy $\alpha^{N-1} \equiv 1 \pmod N$, every y-smooth integer in $[1, p-1]$ lies modulo p in $H_p := \{x \in \mathbb{F}_p^\times : x^{N-1} = 1\}$, of order $\gcd(N-1, p-1) = g$, so $\Psi(p-1,y) \le g$; Lemma 26.1 then gives $g > (p-1)^{3/4}/(\log N)^3$. Finally, for $g \ge N^{5/24}/(2\sqrt{C}(\log N)^3)$, $N^{1/4}/\sqrt{g} \le (2\sqrt{C})^{1/2} N^{7/48} (\log N)^{3/2}$, and trying the $O((\log N)^4)$ bases adds a polylogarithmic factor. □

The bound $N^{1/4}/\sqrt{g}$ therefore holds for every sufficiently large balanced N with $g \le (p-1)^{3/4}/(\log N)^3$. Its exponent is McKee and Pinch's [58, 38]: their rho variant reaches $N^{1/4-\gamma/2}$ in expected time, and what is new here is the deterministic form, with a proven bound and

no knowledge of g. Knowledge of g would do better – $O(N^{1/4-\gamma})$ expected by their babystep–giantstep search [38, Theorem 6.4], polynomial time for $g \geq N^{1/4}$ [38, Theorem 6.3] – but g is a divisor of $N-1$ that the present method never has to find.

27. The Burgess completion

The remaining class $g > (p-1)^{3/4}/(\log N)^3$ is where the smooth-number count fails to supply a non-liar base; a character-sum bound supplies one instead. We use Burgess's bound in the form: for every prime P, every nonprincipal character χ modulo P, every integer $r \geq 1$ and every $x \geq 1$,

$$\left|\sum_{n \leq x} \chi(n)\right| \ll_r \; x^{1-1/r}\, P^{(r+1)/(4r^2)} \log P$$

[11, Theorem 2], with an implied constant depending on r alone; hence for every fixed $\varepsilon > 0$ and $x \geq P^{1/4+\varepsilon}$ (taking $r > 1/(4\varepsilon)$) the sum is $o(x)$ uniformly in χ. The least k-th power non-residue is treated in this uniform way by Norton [66]; we give the short argument in the form needed.

Corollary 27.1 (the large common-factor class)**.** *Fix $C > 1$ and $\varepsilon > 0$. Let $N = pq$ with $p \in J_C$, $p < q$, and $g > (p-1)^{3/4}/(\log N)^3$. Then N is factored deterministically in $O_{C,\varepsilon}(N^{1/(8\sqrt{\mathrm{e}})+\varepsilon})$ bit operations. Consequently, for every sufficiently large balanced semiprime with*

$$g \;\geq\; \frac{N^{5/24}}{2\sqrt{C}\,(\log N)^3},$$

factoring costs $N^{7/48+o(1)}$ or $O_{C,\varepsilon}(N^{1/(8\sqrt{\mathrm{e}})+\varepsilon})$ bit operations; since $1/(8\sqrt{\mathrm{e}}) = 0.0758\ldots < 7/48 < 1/5$, choosing $\varepsilon < 1/5 - 1/(8\sqrt{\mathrm{e}})$ puts both below $N^{1/5}$.

Proof. The subgroup $H_p := \{x \in \mathbb{F}_p^\times : x^{N-1} = 1\}$ has order $\gcd(N-1, p-1) = g$ and index k; since $\mathbb{F}_p^\times$ is cyclic and $k \mid p-1$, it is the subgroup of k-th powers, and likewise H_q has index l. As $p \neq q$, not both indices are 1; let $P \in \{p, q\}$ be a prime whose subgroup H_P has index $h \geq 2$. The indicator of H_P on $\mathbb{F}_P^\times$ is $\frac{1}{h}\sum_\chi \chi$ over the h characters with $\chi^h = 1$, so for $x \geq P^{1/4+\varepsilon}$ the number of integers in $[1, x]$ lying in H_P modulo P is $x/h + o(x)$ by Burgess's bound, uniformly in h (the $h-1$ nonprincipal sums are each $o(x)$ and are divided by h). Fix u with $1 < u < \sqrt{\mathrm{e}}$ and put $y := x^{1/u}$. If every prime $\leq y$ lay in H_P, so would every y-smooth integer, and then $\Psi(x, y) \leq x/h + o(x) \leq x/2 + o(x)$; but $\Psi(x, x^{1/u}) = (\rho(u) + o(1))x$ [80, Chapter III.5] with $\rho(u) = 1 - \log u > 1/2$ for $1 < u < \sqrt{\mathrm{e}}$, a contradiction for x large. Hence some prime $\alpha \leq y = P^{(1/4+\varepsilon)/u}$ lies outside H_P, i.e. $\alpha^{N-1} \not\equiv 1 \pmod P$ and so $\beta := \alpha^{N-1} \not\equiv 1 \pmod N$; letting $u \uparrow \sqrt{\mathrm{e}}$ and using $P = \Theta_C(N^{1/2})$, some $\alpha \leq N^{1/(8\sqrt{\mathrm{e}})+\varepsilon'}$ qualifies for every $\varepsilon' > 0$ and N large in terms of C and ε'. Enumerate the bases up to this bound, computing $\gcd(\alpha, N)$ and β, and skip those with $\beta \equiv 1$; for the first remaining base the collision search of Lemma 26.2 factors N in $O(\sqrt{\min(k,l)})(\log N)^{O(1)}$ operations, and here $\min(k,l) = k < (p-1)^{1/4}(\log N)^3$ because $k < l$, so this is $N^{1/16+o(1)}$, dominated by the enumeration since $1/(8\sqrt{\mathrm{e}}) > 1/16$. The second statement combines this with Lemma 26.2. □

Remark 27.2 (direct enumeration). In the class of Corollary 27.1 a direct enumeration is also available but slower: $l/k = (q-1)/(p-1) \leq C(1+o(1))$, so $l \leq 2Ck$ for N large, and from $N - 1 = (k+l)g + klg^2$ one has $4kl(N-1) + (k+l)^2 = (2klg + k + l)^2$. Whenever $(k+l)^2 < 4klg + 2(k+l) - 1$ this gives $2klg + k + l = \lfloor\sqrt{4kl(N-1)}\rfloor + 1$, and the inequality holds throughout the class for N large, since $(k+l)^2 \leq (1+2C)^2k^2 \leq 4klg$ as soon as $g \geq (1+2C)^2/4$. So one square test per coprime pair (k, l) with $k < (p-1)^{1/4}(\log N)^3$ recovers g, p and q in $N^{1/4+o(1)}$ operations.

28. A deterministic curve for the class

Lemma 26.2 and Corollary 27.1 give the exponent $1/4-\gamma/2$ for $g=N^\gamma$ without knowledge of g; it is below $1/5$ for $\gamma>1/10$. Two further routes, both elementary once a common divisor of $p-1$ and $q-1$ is known and both known in that form, combine with a deterministic recovery of that divisor from $N-1$ into a curve below $1/5$ for every $\gamma>1/20$.

The Fermat progression. Let g' be any common divisor of $p-1$ and $q-1$ and write $p=1+g'x$, $q=1+g'y$. Then $N-1=g'(x+y)+g'^2xy$, so $M':=(N-1)/g'$ is an integer with $x+y\equiv M'\pmod{g'}$; with $c:=M' \bmod g'$ and $x+y=c+g't$,

$$p+q=r+g'^2t,\qquad r:=2+g'c,\qquad t\ge 0. \tag{1}$$

For balanced p,q with $q/p<C$ the sum $S:=p+q$ lies in $[\lceil 2\sqrt{N}\rceil,\lfloor K_C\sqrt{N}\rfloor]$, $K_C:=\sqrt{C}+1/\sqrt{C}$, so t lies in $[t_-,t_+]$ with $t_-:=\max\{0,\lceil(\lceil 2\sqrt{N}\rceil-r)/g'^2\rceil\}$ and $t_+:=\lfloor(\lfloor K_C\sqrt{N}\rfloor-r)/g'^2\rfloor$, and the number of candidates is $n(g'):=t_+-t_-+1\le (K_C-2)\sqrt{N}/g'^2+2$. Neither $g'=\gcd(p-1,q-1)$ nor $\gcd(x,y)=1$ is used.

Lemma 28.1 (the Fermat cell)**.** *For every integer α, $\alpha^{p+q}\equiv\alpha^{N+1}\pmod N$.*

Proof. Modulo p, $\alpha^p\equiv\alpha$ gives $\alpha^{p+q}\equiv\alpha^{q+1}$ and $\alpha^{pq+1}=(\alpha^p)^q\alpha\equiv\alpha^{q+1}$; symmetrically modulo q; combine by the Chinese remainder theorem. □

This is Harvey's cell $(a,b)=(1,1)$ [31], for which the congruence holds modulo both primes at once.

Proposition 28.2 (a deterministic curve for the common-factor class)**.** *Fix $C>1$. Every balanced $N=pq$ with distinct odd primes and $g:=\gcd(p-1,q-1)=N^\gamma$ is factored deterministically from N alone in $N^{E(\gamma)+o(1)}$ bit operations, where*

$$E(\gamma)=\begin{cases}1/4-\gamma & 0\le\gamma\le 1/12,\\ 1/8+\gamma/2 & 1/12\le\gamma\le 1/8,\\ 1/4-\gamma/2 & 1/8\le\gamma\le 1/6,\\ 1/2-2\gamma & 1/6\le\gamma\le 1/5,\\ \gamma/2 & 1/5\le\gamma\le 1/4,\\ 1/4-\gamma/2 & 1/4\le\gamma<3/8,\\ 1/(8\sqrt{\mathrm{e}})+\varepsilon & 3/8\le\gamma<1/2,\end{cases}$$

for every fixed $\varepsilon>0$ in the last branch, with implied constants depending on C and ε; the $N^{o(1)}$ is the divisor count $d(N-1)$. In particular $E(\gamma)<1/5$ for every $\gamma>1/20$, while $1/4-\gamma/2$ is below $1/5$ only for $\gamma>1/10$; the deterministic record for the class is $\min\{1/5,E(\gamma)\}$ [31]. The curve is not monotone: its maximum over $\gamma\ge\gamma_0$ is $1/4-\gamma_0$ for $\gamma_0\le 1/16$ and $3/16$ for $1/16\le\gamma_0\le 1/8$.

Proof. Three routes are run together with the dovetailing described at the end, so the algorithm needs neither g nor γ.

Route A is Lemma 26.2 with Corollary 27.1, whose cost is

$$O(N^{1/4-\gamma/2})(\log N)^{O(1)} \quad \text{when } g\le(p-1)^{3/4}/(\log N)^3, \text{ i.e. for every fixed } \gamma<3/8,$$
$$O_{C,\varepsilon}\big(N^{\max\{1/4-\gamma/2,\ 1/(8\sqrt{\mathrm{e}})\}+\varepsilon}\big) \quad \text{in general,}$$

the second exponent being the Burgess base search; for $\gamma\ge 3/8$ that is the last branch (at $\gamma=3/8$ itself $g=N^{3/8}$ exceeds $(p-1)^{3/4}/(\log N)^3$ by the logarithmic factor, so the general bound is the one that applies).

Route B (given a common divisor $g' \le N^{1/4}$). Let $n := n(g')$, $m := \lceil\sqrt{n}\rceil$ and $S_0 := r + g'^2 t_-$, and let α be a unit modulo N with $\mathrm{ord}_N(\alpha) > g'^2 m$: Harvey and Hittmeir [33, Theorem 1.1] supply it, or factor N, for $D := g'^2 m$, which satisfies $1 \le D < N-1$ for N large since $D = O_C(g'N^{1/4}) = O_C(N^{1/2})$, at cost $O(\sqrt{D})(\log N)^{O(1)} = O_C(N^{1/8}\sqrt{g'})(\log N)^{O(1)}$. Put $\beta := \alpha^{g'^2}$ and $\eta := \alpha^{N+1-S_0} \bmod N$. By Lemma 28.1 the true shifted index $u := t - t_- \in [0, n)$ satisfies $\beta^u \equiv \eta \pmod N$. Compute the babies β^i, $0 \le i < m$, and the giants $\eta\beta^{-mk}$, $0 \le k < \lceil n/m\rceil$, sort them and match modulo N; a match (i, k) with $u = i + mk < n$ gives $S = S_0 + g'^2 u$, accepted if and only if $S^2 - 4N$ is a perfect square, in which case $p, q = (S \mp \sqrt{S^2 - 4N})/2$. Since $\mathrm{ord}_N(\beta) \ge \mathrm{ord}_N(\alpha)/g'^2 > m$, the babies are pairwise distinct modulo N, each giant matches at most one baby, and the matched u form the residue class of the true one modulo $\mathrm{ord}_N(\beta)$ intersected with $[0, n)$ – at most $n/m + 1 \le m + 1$ of them, each tested in $O(1)$ operations. The cost is $O(m + n/m) = O_C(N^{1/4}/g')$ group operations plus the selection, i.e. $N^{\max\{1/4-\gamma',\ 1/8+\gamma'/2\}+o(1)}$ for $g' = N^{\gamma'}$.

Route C (given g'). For $t = t_-, \dots, t_+$ put $s := c + g't$ and $xy := (M' - s)/g'$, and accept t if and only if $z^2 - sz + xy$ has integer roots x, y with $1 + g'x$ dividing N; $O(1)$ operations per trial, $O_C(\sqrt{N}/g'^2 + 1)$ in all. For $g' \ge N^{1/4}$ there are $O_C(1)$ candidates, and when $g' > x + y$ there is one: Hinek's Theorem 6.3 [38] in this notation.

Finding g. Every prime factor of g is at most g. For a bound B, Pollard–Strassen [69, 78] computes the B-smooth part of $N - 1$ with its factorisation in $O(\sqrt{B})(\log N)^{O(1)}$ operations, and g divides it once $B \ge g$; its divisors number at most $d(N-1) = N^{o(1)}$. Dovetail on a budget 2^j, $j = 1, 2, \dots$: for every dyadic range $[2^s, 2^{s+1})$ whose cost bound,

$$\begin{aligned} &\max\{N^{1/4}/2^s,\ N^{1/8}2^{(s+1)/2},\ 2^{(s+1)/2}\} && \text{for Route B, when } 2^s \le N^{1/4},\\ &\max\{\sqrt{N}/4^s + 1,\ 2^{(s+1)/2}\} && \text{for Route C,} \end{aligned}$$

is at most 2^j (candidates above $N^{1/4}$ in the range straddling $N^{1/4}$ are passed to Route C), compute the 2^{s+1}-smooth part of $N - 1$ and run the route on every divisor g' of it in the range, interleaving the steps of Route A. Every output is verified, so a false candidate cannot return a false factor. The work at budget j is $O(\log N)\, d(N-1)\, 2^j (\log N)^{O(1)} = N^{o(1)}2^j$, the budgets double, and the range containing g is run as soon as 2^j exceeds its cost bound; the total is therefore $N^{o(1)}$ times the least of the three routes' costs at γ. That minimum is $E(\gamma)$: Route A gives $1/4 - \gamma/2$ for $\gamma < 3/8$ and the plateau from $3/8$ on; Route B gives $\max\{1/4 - \gamma,\ 1/8 + \gamma/2\}$ for $\gamma \le 1/4$; Route C gives $\max\{\gamma/2,\ 1/2 - 2\gamma\}$ with $1/2 - 2\gamma$ read as 0 for $\gamma \ge 1/4$, the $\gamma/2$ being the smooth-part cost; the breakpoints are $1/12$, $1/8$, $1/6$, $1/5$ and $1/4$, where consecutive branches agree, and $3/8$, where the curve steps up from $1/16$ to the plateau $1/(8\sqrt{\mathrm{e}}) = 0.0758\dots$. □

What is new here. The known-g exponent $1/4 - \gamma$ of Route B is McKee and Pinch's [58], as restated in [38, Theorem 6.4], and the progression (1) is elementary; Route C for $g \ge N^{1/4}$ is [38, Theorem 6.3]; the order selection is Harvey and Hittmeir's; Pollard–Strassen and divisor enumeration are standard. What we have not found stated is the composition: the progression search realised as an exact babystep–giantstep collision, the recovery of g from the smooth part of $N - 1$ inside the same budget – Hinek [38, §6.3.4] seeks g by the elliptic curve method or the number field sieve – and the resulting N-only curve, obtained with no knowledge of γ. Route B does not realise the known-g exponent for every γ: the order selection dominates for $\gamma > 1/12$.

29. An implementation check

The collision search of Lemma 26.2 was implemented as stated – the doubling bounds $D' = 4, 16, \dots$ with $H = \lfloor\sqrt{D'}\rfloor + 1$ babies and $\lceil D'/H\rceil$ giants, exact-order recovery from an exact

$\Lambda_d(P_{\min})$ 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