PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

A Hyperelliptic Smoothness Test. I

H. W. Lenstra, J. Pila and Carl Pomerance

Phil. Trans. R. Soc. Lond. A 1993 **345**, 397-408
doi: 10.1098/rsta.1993.0138

A hyperelliptic smoothness test. I

By H. W. Lenstra Jr[1], J. Pila[2] and Carl Pomerance[3]

[1] *Department of Mathematics, University of California, Berkeley, California 94720, U.S.A.*

[2] *6 Goldthorns Avenue, Kew 3101, Australia*

[3] *Department of Mathematics, University of Georgia, Athens, Georgia 30602, U.S.A.*

This series of papers is concerned with a probabilistic algorithm for finding small prime factors of an integer. While the algorithm is not practical, it yields an improvement over previous complexity results. The algorithm uses the jacobian varieties of curves of genus 2 in the same way that the elliptic curve method uses elliptic curves. In this first paper in the series a new density theorem is presented for smooth numbers in short intervals. It is a key ingredient of the analysis of the algorithm.

1. Introduction

In this series of papers we present a probabilistic algorithm for finding small prime factors of an integer. It may be used to detect and factor smooth numbers. We call our algorithm the *hyperelliptic curve method*, as it uses the jacobian varieties of curves of genus 2 over finite fields in the same way that the elliptic curve method (Lenstra 1987) uses elliptic curves over finite fields.

For real numbers a, b and x with $x > \mathrm{e}$ set

$$L_x[a,b] = \exp\left(b(\log x)^a (\log\log x)^{1-a}\right).$$

Theorem 1.1. *There are effectively computable positive constants c_0, n_0 with the following property. Given an integer $n \geqslant n_0$ that is not a prime power, the hyperelliptic curve method obtains a non-trivial divisor of n in expected time at most*

$$L_p[\tfrac{2}{3}, c_0](\log n)^2,$$

where p is the least prime divisor of n.

The run time is measured in bit operations. Our definitions of *probabilistic algorithm* and *expected time* are as given by Lenstra & Pomerance (1992).

Corollary 1.2. *There is a probabilistic algorithm with the following property. Given integers $n \geqslant n_0$ and $v \geqslant 3$, the algorithm runs in time at most*

$$L_v[\tfrac{2}{3}, c_0](\log n)^3,$$

and obtains, with probability at least $\frac{1}{2}$, all prime factors p of n with $p \leqslant v$.

The hyperelliptic curve method is of purely theoretical interest; the following comparisons with other methods are on a theoretical basis only.

The deterministic algorithm of Pollard (1974) and Strassen (1977), also described in Pomerance (1982), was heretofore the best algorithm known for finding all prime

Phil. Trans. R. Soc. Lond. A (1993) **345**, 397–408
Printed in Great Britain

factors $\leqslant v$ of a number n. It remains the best deterministic algorithm for this purpose, running in time

$$O(\sqrt{v}(\log v)^2 \log n \log\log n \log\log\log n).$$

Their method is based on fast multiplication techniques; if these are used in the hyperelliptic curve method, then the factor $(\log n)^2$ in Theorem 1.1 may be replaced by $(\log n)^{1+o(1)}$, for $n \to \infty$.

If v is very small as a function of n, then the algorithm of Pollard and Strassen remains faster than the hyperelliptic curve method. At the other extreme, if v is relatively large, it is better to use a factoring algorithm that is insensitive to the size of the factors. Specifically, the class group relations method (see Lenstra & Pomerance 1992) is faster than the hyperelliptic curve method if v is of order at least $L_n[\frac{3}{4}, 2c_0^{-\frac{3}{2}}/\sqrt{3} + o(1)]$ for $n \to \infty$.

Conjecturally, the hyperelliptic curve method is not as good as the elliptic curve method. Under a reasonable hypothesis concerning the distribution of smooth numbers in short intervals, the expected run time of the elliptic curve method is at most

$$L_p[\tfrac{1}{2}, \sqrt{2} + o(1)]\,(\log n)^2,$$

where n is the number being factored, p its least prime divisor, and the $o(1)$ is for $p \to \infty$. Under a similar hypothesis, the expected run time of the hyperelliptic curve method, with optimal choice of parameters, is actually at most

$$L_p[\tfrac{1}{2}, 2 + o(1)]\,(\log n)^2,$$

with n, p and $o(1)$ as above.

The algorithm of Corollary 1.2 may be used to recognize, with high probability, numbers that are v-smooth, i.e. built up from prime factors less than or equal to v. Smooth numbers play an important role in many algorithms that have been proposed for the discrete logarithm problem and for factoring integers (see Lenstra & Lenstra 1990). Our results may contribute to the run time analysis of such algorithms. So far it has sufficed to use the elliptic curve method for this purpose: while it has not been proved to recognize all smooth numbers, it does recognize many of them (see Pomerance 1987; Lenstra & Pomerance 1992).

The relationship between the elliptic and the hyperelliptic methods has an antecedent in primality testing. The *random curve* primality test of Goldwasser & Kilian (1986) proceeds by choosing a random elliptic curve E over $\boldsymbol{Z}/p\boldsymbol{Z}$, where p is the number being tested. They prove that their method runs in 'random polynomial time' for most primes p. The same result for all primes is conditional on a standard conjecture regarding the density of primes in short intervals, specifically of the form $[x, x + c\sqrt{x}]$; the order of the group $E(\boldsymbol{Z}/p\boldsymbol{Z})$ of rational points of E over $\boldsymbol{Z}/p\boldsymbol{Z}$ belongs to such an interval, with $x \approx p$, if p is prime. In the *abelian variety* primality test of Adleman & Huang (1987, 1992), the elliptic curve is replaced by the jacobian J of a curve of genus 2, which is a two-dimensional abelian variety. If p is prime, the order of $J(\boldsymbol{Z}/p\boldsymbol{Z})$ belongs to an interval of the form $[x, x + cx^{\frac{3}{4}}]$, with $x \approx p^2$, and the analysis depends on the density of primes in intervals of that form. Such intervals are not so short: a known density theorem enables Adleman & Huang to prove unconditionally that all prime numbers can be recognized in random polynomial time.

The idea of using jacobians of curves of genus 2 in place of elliptic curves in the present context of factoring was inspired by the work just mentioned of Adleman &

Huang. Now the analysis hinges on the density of smooth numbers – as opposed to prime numbers – in intervals of the same form. For the elliptic curve method, no adequate density result is available; for the hyperelliptic curve method we are able to supply one.

Theorem 1.3. *Let* $c_1 = (1\,980\,000)^{\frac{1}{3}}$. *There is an effectively computable constant* x_3 *such that if* $x \geqslant x_3$, $z = L_x[\frac{2}{3}, c_1]$, *and* $x^{\frac{3}{5}} \leqslant y \leqslant x$, *then the number of* z*-smooth integers in the interval* $[x, x+y]$ *is at least* $y \cdot \exp(-(\log x)^{\frac{1}{3}} (\log\log x)^{\frac{8}{3}})$.

This first paper in the series is devoted to the proof of Theorem 1.3. Our proof will follow the same general lines as that of Harman (1991), who showed that if $\epsilon > 0$ is arbitrary and $z = \exp((\log x)^{\frac{2}{3}+\epsilon})$, $y = x^{\frac{1}{2}+\epsilon}$, then there is at least one z-smooth integer in the interval $[x, x+y]$ once x is sufficiently large depending on the choice of ϵ. Harman's proof is in turn a refinement of an argument of Balog (1987) who showed the same result but with $z = x^{\epsilon}$. Friedlander & Granville (this volume) obtain an asymptotic result for the number of z-smooth integers in the interval $[x, x+y]$ when $y = x^{\frac{1}{2}} z^{2+\epsilon}$ and $z \geqslant \exp((\log x)^{\frac{5}{6}+\epsilon})$.

In §2 we state a result more general than Theorem 1.3 and give a few lemmas. In §3 we use a combinatorial argument to reduce the proof to the estimation of a certain weighted sum. In §4 this estimation is carried out by an analytic argument. The proof that Theorem 1.3 follows from the more general result stated in §2 is given at the end of §4.

2. Smooth numbers in short intervals

If x, z are real numbers, let $\psi(x, z)$ denote the number of positive z-smooth integers $\leqslant x$. If $e \leqslant z \leqslant x$, let

$$u = u(x, z) = (\log x)/\log z, \quad \alpha = \alpha(x, z) = (\log\log z)/\log\log x.$$

It is known (see Canfield *et al.* 1983) that if $\exp((\log x)^{\epsilon}) \leqslant z \leqslant x^{1-\epsilon}$, then

$$\psi(x, z) = x \cdot \exp(-u(\log u + \log\log u + O_{\epsilon}(1))).$$

(In fact an asymptotic formula is known in this range.) Thus if the z-smooth numbers $\leqslant x$ are not too wildly distributed, then we might expect, for numbers y with $\sqrt{x} \leqslant y \leqslant x$, that

$$\psi(x+y, z) - \psi(x, z) = y \cdot \exp(-u(\log u + \log\log u + O_{\epsilon}(1))). \tag{2.1}$$

The following theorem is a step in this direction.

Theorem 2.1. *There are effectively computable positive constants* x_0, c_1, c_2, c_3 *and* c_4, *such that in the range*

$$x \geqslant x_0, \quad L_x[\tfrac{3}{4}, c_2] \leqslant z \leqslant \exp((\log x)/\log\log x), \quad \sqrt{(xz)} \leqslant y \leqslant x, \tag{2.2}$$

we have

$$\psi(x+y, z) - \psi(x, z) \geqslant y \cdot \exp(-u(\log u + \log\log u + c_3)); \tag{2.3}$$

in the range

$$\left.\begin{aligned} x \geqslant x_0, \quad & \exp((\log x \log\log x)^{\frac{2}{3}}) \leqslant z \leqslant L_x[\tfrac{3}{4}, c_2], \\ & x^{\frac{1}{2}} \exp(2c_4 u^3 \log u) \leqslant y \leqslant x, \end{aligned}\right\} \tag{2.4}$$

we have

$$\psi(x+y, z) - \psi(x, z) \geqslant y \cdot \exp\left(-\left(1 + 48\frac{3-4\alpha}{3\alpha-2}\right) u \log u - \frac{18}{3\alpha-2} u \log\log u\right); \tag{2.5}$$

and in the range

$$\left.\begin{array}{l} x \geqslant x_0, \quad L_x[\frac{2}{3}, c_1] \leqslant z \leqslant \exp((\log x \log\log x)^{\frac{2}{3}}), \\ x^{\frac{1}{2}} \exp(c_4 u^3 \log u) \leqslant y \leqslant x, \end{array}\right\} \tag{2.6}$$

we let β *be such that* $z = \exp((\log x)^{\frac{2}{3}} (\log\log x)^{\beta})$ *and we have*

$$\psi(x+y, z) - \psi(x, z) \geqslant y \cdot \exp(-21u(\log u)^{4-3\beta} (\log\log u)^{-1}). \tag{2.7}$$

Furthermore, the expression $x^{\frac{1}{2}} \exp(c_4 u^3 \log u)$ *does not exceed* $x^{\frac{3}{5}}$ *if* (2.6) *holds.*

We shall only be applying the range (2.6) to the analysis of the algorithm, and then only in the case $z = L_x[\frac{2}{3}, c_1]$. However, it is little extra work to prove the full Theorem 2.1.

In our proof below, the constants implied by the notation O and the notation $\ll$ shall always be absolute. If $\mathscr{N}$ is a finite set of positive integers and s is a complex number, we denote by $\mathscr{N}(s)$ the Dirichlet polynomial $\Sigma_{n \in \mathscr{N}} n^{-s}$.

We now state some lemmas. For a complex number s, we denote by σ the real part of s and by t the imaginary part.

Lemma 2.8. *There are effectively computable positive constants* x_1, c_5, c_6, *such that if* L *is a real number with* $L \geqslant x_1$ *and* $\mathscr{L}(s)$ *is the function* $\Sigma_{L < l \leqslant \mathrm{e}L} l^{-s}$, *then in the range* $\frac{1}{2} \leqslant \sigma \leqslant 1$,

$$|\mathscr{L}(s)| \leqslant c_5 L^{1-\sigma} \left(\frac{1}{1+|t|} + \exp\left(-c_6 \frac{(\log L)^3}{(\log(2+|t|))^2} \right) \right).$$

This result follows from the proof of Lemma 2 in Harman (1991). Namely, a trivial estimate is used for $|t| \leqslant L$, an estimate of van der Corput type is used for $L \leqslant |t| \leqslant L^{19}$, and the remaining range follows from estimates of Korobov and Vinogradov. We may take 1/60000 as a value for c_6 in Lemma 2.8. This number is stated as a valid choice for c_6 in Harman (1991) for the range $|t| \geqslant L^{19}$. A valid choice for c_6 in the van der Corput range $L \leqslant |t| \leqslant L^{19}$ is 1/3000. (Thanks are due to S. W. Graham for informing us of this latter fact.)

Lemma 2.9. *There is an effectively computable positive constant* c_7 *such that if* U *is a positive real number,* J *is a positive integer and* $b_1, \ldots, b_J$ *are complex numbers, then*

$$\int_0^U \left| \sum_{j=1}^{J} b_j j^{\mathrm{i}t} \right|^2 \mathrm{d}t \leqslant c_7 (U+J) \sum_{j=1}^{J} |b_j|^2.$$

This result is Theorem 6.1 in Montgomery (1971).

Let $\Omega(N)$ denote the number of prime factors of N counted with multiplicity.

Lemma 2.10. *There are effectively computable positive constants* x_2, c_8 *such that if* L, Λ *are numbers satisfying* $L \geqslant x_2$, $(2\mathrm{e}\log\log L)^{\frac{3}{2}} \leqslant \Lambda \leqslant \log L$ *and* $\mathscr{L}$ *is the set of integers* l *satisfying*

(i) $L < l \leqslant \mathrm{e}L$,
(ii) l *is free of prime factors below* $\log L / \log\log L$,
(iii) $\Omega(l) \leqslant \Lambda$,

then in the range $\frac{1}{2} \leqslant \sigma \leqslant 1$,

$$|\mathscr{L}(s)| \leqslant c_8 L^{1-\sigma} (\log\log L) \left(\frac{1}{1+|t|} + \exp\left(-\tfrac{4}{5} c_6 \frac{(\log L)^3}{(\log(2+|t|))^2} \right) + \frac{1}{\Lambda^{\Lambda/3}} \right).$$

Proof. Let $\mathscr{L}_0$ be the set of integers l satisfying conditions (i) and (ii). Let P denote the product of the primes below $w = \log L/\log\log L$. Then

$$\mathscr{L}_0(s) = \sum_{\substack{L<l\leqslant \mathrm{e}L\\(l,P)=1}} l^{-s} = \sum_{d|P}\mu(d)\sum_{\substack{L<l\leqslant \mathrm{e}L\\ d|l}} l^{s} = \sum_{d|P}\mu(d)\,d^{-s}\sum_{L|d<l\leqslant \mathrm{e}L/d} l^{-s}.$$

Thus

$$|\mathscr{L}_0(s)| \leqslant \sum_{d|P} d^{-\sigma}\left|\sum_{L/d<l\leqslant \mathrm{e}L/d} l^{-s}\right|. \tag{2.11}$$

Note that $P = \exp(O(\log L/\log\log L)) = L^{O(1/\log\log L)}$. We suppose x_2 is so large that $P \leqslant L^{1/20}$ and $L/P \geqslant x_1$. We have from (2.11) and Lemma 2.8 that

$$\begin{aligned}|\mathscr{L}_0(s)| &\leqslant c_7\sum_{d|P} d^{-\sigma}(L/d)^{1-\sigma}\left(\frac{1}{1+|t|}+\exp\left(-c_6\frac{(\log(L/d))^3}{(\log(2+|t|))^2}\right)\right)\\ &\leqslant c_7 L^{1-\sigma}\left(\frac{1}{1+|t|}+\exp\left(-\tfrac{4}{5}c_6\frac{(\log L)^3}{(\log(2+|t|))^2}\right)\right)\sum_{d|P} d^{-1}\\ &\leqslant c_9 L^{1-\sigma}\left(\frac{1}{1+|t|}+\exp\left(-\tfrac{4}{5}c_6\frac{(\log L)^3}{(\log(2+|t|))^2}\right)\right)\log\log L\end{aligned} \tag{2.12}$$

for some absolute positive constant c_9.

Let $\mathscr{L}_1$ denote the set of $l\in\mathscr{L}_0$ for which condition (iii) fails. Then

$$|\mathscr{L}(s)| = |\mathscr{L}_0(s)-\mathscr{L}_1(s)| \leqslant |\mathscr{L}_0(s)|+|\mathscr{L}_1(s)|. \tag{2.13}$$

We now estimate $|\mathscr{L}_1(s)|$. We have for any real number $v \geqslant 1$,

$$\begin{aligned}\mathscr{L}_1(1) &= \sum_{l\in\mathscr{L}_1}\frac{1}{l} \leqslant v^{-\Lambda}\sum_{l\in\mathscr{L}_1}\frac{v^{\Omega(l)}}{l}\\ &\leqslant v^{-\Lambda}\sum_{p|l\Rightarrow w<p\leqslant \mathrm{e}L}\frac{v^{\Omega(l)}}{l} = v^{-\Lambda}\prod_{w<p\leqslant \mathrm{e}L}\left(1+\frac{v}{p}+\frac{v^2}{p^2}+\ldots\right).\end{aligned}$$

Thus if $1 \leqslant v \leqslant \frac{1}{2}w$,

$$\mathscr{L}_1(1) \leqslant v^{-\Lambda}\prod_{w<p\leqslant \mathrm{e}L}\left(1+\frac{2v}{p}\right) \leqslant v^{-\Lambda}\exp\left(\sum_{w<p\leqslant \mathrm{e}L}\frac{2v}{p}\right) \leqslant v^{-\Lambda}\exp(2v\log\log L), \tag{2.14}$$

if x_2 is sufficiently large. Letting $v = \Lambda/(2\log\log L)$, we have $1 \leqslant v \leqslant \frac{1}{2}w$. Thus from (2.14) and our hypothesis we have

$$|\mathscr{L}_1(s)| \leqslant (\mathrm{e}L)^{1-\sigma}\,\mathscr{L}_1(1) \leqslant (\mathrm{e}L)^{1-\sigma}\,\Lambda^{-\Lambda}(2\mathrm{e}\log\log L)^{\Lambda} \leqslant (\mathrm{e}L)^{1-\sigma}\,\Lambda^{-\Lambda/3}$$

and Lemma 2.10 now follows from (2.12) and (2.13). □

3. A combinatorial beginning

In this section we begin the proof of Theorem 2.1. Suppose x is a large number (how large will be determined as we proceed) and suppose z is a number in the range $L_x[\frac{2}{3},1] \leqslant z \leqslant \exp(\log x/\log\log x)$. We thus have the numbers u, α determined by the equations $z = x^{1/u} = \exp((\log x)^{\alpha})$. Let L, k, M be given as follows:

$$L = z^{\frac{1}{2}},\quad k = \left[\frac{24}{c_6}\cdot\frac{u^3\log u}{\log z}\right],\quad M = x^{\frac{1}{2}}L^{-(k+1)/2}, \tag{3.1}$$

where c_6 is the constant introduced in Lemma 2.8. We shall choose the constant c_2 in (2.2) so that $c_2 = (6/c_6)^{\frac{1}{4}}$ which implies that $k = 1$ for z in the range (2.2). We shall choose y so that

$$y = x/M = x^{\frac{1}{2}}L^{(k+1)/2}. \tag{3.2}$$

In addition, we shall choose the constant c_4 in (2.4), (2.6) so that $c_4 = 9/c_6$. Note that if $k \geqslant 2$, then

$$k+1 < \frac{72}{c_6}\cdot\frac{u^3 \log u}{\log z},$$

so that $L^{(k+1)/2} < \exp((18/c_6)u^3 \log u) = \exp(2c_4 u^3 \log u)$. Also note that in the range (2.6), we have

$$k+1 < \frac{25}{c_6}\cdot\frac{u^3 \log u}{\log z}$$

for x sufficiently large, so that $L^{(k+1)/2} < \exp(c_4 u^3 \log u)$. Thus the value of y given by (3.2) is slightly smaller than the lower bound specified for y in (2.4) and (2.6) and is exactly equal to the lower bound for y in (2.2). Proving the theorem for y given by (3.2) is thus sufficient to establish the theorem in general.

We shall choose the constant c_1 in (2.6) so that $c_1 = (33/c_6)^{\frac{1}{3}}$. A simple calculation shows that for all sufficiently large x and $z \geqslant L_x[\frac{2}{3}, c_1]$ we have $x^{\frac{1}{2}} \exp(c_4 u^3 \log u) \leqslant x^{\frac{3}{5}}$, which is one of the assertions of Theorem 2.1.

Let $\mathscr{M}$ be the set of integers m with $M < m \leqslant eM$ such that every prime factor p of m is in the range $eL < p \leqslant z$. Let

$$v = \log M/\log z = \tfrac{1}{2}u - \tfrac{1}{4}(k+1). \tag{3.3}$$

From our choice of c_1 we have for all sufficiently large x that

$$k+1 < \tfrac{1}{4}u. \tag{3.4}$$

From (1.7) in Theorem 2 in Saias (1993) and from Theorem 1 and (iv), (v) of Lemma 4 in Saias (1992) (cf. Theorem 6 of Friedlander 1976) we have

$$\mathscr{M}(1) = \sum_{m\in\mathscr{M}} m^{-1} = \exp(-v \log v - v \log\log v + O(v)).$$

Thus

$$\mathscr{M}(1)^2 = \exp(-(u - \tfrac{1}{2}k)(\log u + \log\log u + O(1))). \tag{3.5}$$

We now give three definitions of a set $\mathscr{L}$ of integers depending on the three ranges for z in Theorem 2.1. If z is in the range specified in (2.2), we let $\mathscr{L}$ be the set of integers l with $L < l \leqslant eL$. If z is in the range specified in (2.4), we let $\mathscr{L}$ be the set of integers described in Lemma 2.10 where Λ satisfies

$$\Lambda \log \Lambda = \tfrac{1}{2}c_6 \cdot (\log z)/u^2. \tag{3.6}$$

Finally if z is in the range specified in (2.6), we let $\mathscr{L}$ be the set of integers described in Lemma 2.10 where Λ satisfies

$$\Lambda \log \Lambda = \tfrac{1}{2}c_6 (\log\log x)^2. \tag{3.7}$$

Let $\mathscr{S}(x, z)$ denote the set of ordered $(k+3)$-tuples $(m, n, r, l_1, \ldots, l_k)$ where $m, n \in \mathscr{M}$, $l_1, \ldots, l_k \in \mathscr{L}$, r is a prime or prime power and $mnrl_1 \cdots l_k \leqslant x + y$. Since by (3.1)

$$r \leqslant \frac{x+y}{mnl_1\cdots l_k} \leqslant \frac{x+y}{M^2L^k} \leqslant \frac{2x}{M^2L^k} = 2L,$$

the product N of the entries of any element of $\mathscr{S}(x,z)$ is a z-smooth integer. For any integer N, let $R_{x,z}(N)$ denote the number of $(m,n,r,l_1,\dots,l_k)\in\mathscr{S}(x,z)$ with $N=mnrl_1\cdots l_k$. For any positive integer N there is a unique factorization $N=N_1N_2$, where each prime factor of N_1 exceeds eL and each prime factor of N_2 is at most eL. Thus if $(m,n,r,l_1,\dots,l_k)\in\mathscr{S}(x,z)$ and $N=mnrl_1\cdots l_k$, then $N_1=mn$ and $N_2=rl_1\cdots l_k$. We conclude that $R_{x,z}(N)$ is at most the number of ordered factorizations of N_1 as a product of two positive integers times the number of ordered factorizations of N_2 as a product of a prime or prime power times the product of k positive integers. Further, in the ranges (2.4) and (2.6), each of these k positive integers has at most Λ prime factors. That is,

$$R_{x,z}(N)\leqslant d_2(N_1)\sum_{r\mid N_2,\,\Omega(N_2/r)\leqslant k\Lambda}{}'\, d_k(N_2/r), \tag{3.8}$$

where $d_j(w)$ is the number of ordered factorizations of the positive integer w into j positive integers (so that d_2 is the well-known divisor function), where r runs over primes and prime powers and where the dash indicates that there is no restriction on $\Omega(N_2/r)$ when z is in the range (2.2). Since $d_j(w)\leqslant j^{\Omega(w)}$, we have from (3.8) and the fact that $k=1$ in the range (2.2) that

$$R_{x,z}(N)\leqslant\begin{cases}2^{\Omega(N_1)}\Omega(N_2), & \text{if (2.2) holds,}\\ 2^{\Omega(N_1)}\Omega(N_2)k^{k\Lambda}, & \text{if (2.4) or (2.6) hold.}\end{cases} \tag{3.9}$$

From the definition of $\mathscr{M}$, if $R_{x,z}(N)>0$, then $\Omega(N_1)=O(u)$ so that

$$2^{\Omega(N_1)}\leqslant \mathrm{e}^{O(u)}. \tag{3.10}$$

In addition we have

$$\Omega(N_2)\leqslant\log_2 N_2=O(\log x)=u^{O(1)}. \tag{3.11}$$

In the range (2.2) we have by (3.9)–(3.11) that

$$R_{x,z}(N)\leqslant \mathrm{e}^{O(u)} \tag{3.12}$$

for any integer N.

Suppose now that z is in the range (2.4). From (3.1) we have

$$k\log k\leqslant\frac{48}{c_6}\cdot\frac{u^3\log u}{\log z}(3\log u-\log\log z+\log\log u+O(1)).$$

From (3.6) we have that $\log\log\Lambda$ is small compared with $\log\Lambda$ when x is large, so that

$$\Lambda<c_6\frac{\log z}{u^2(\log\log z-2\log u)}$$

for all large x. Thus using $\log u=(1-\alpha)\log\log x$ and $\log\log z=\alpha\log x$, we have

$$\begin{aligned}k\Lambda\log k&\leqslant 48u\log u\cdot\frac{3\log u-\log\log z+\log\log u+O(1)}{\log\log z-2\log u}\\&=48u\log u\cdot\frac{(3-4\alpha)\log\log x+\log\log u+O(1)}{(3\alpha-2)\log\log x}\\&\leqslant 48\frac{3-4\alpha}{3\alpha-2}u\log u+\frac{16}{3\alpha-2}u\log\log u+O\left(\frac{u}{3\alpha-2}\right).\end{aligned}$$

Hence from (3.9)–(3.11) we have for any integer N,

$$R_{x,z}(N) \leqslant \exp\left(48\frac{3-4\alpha}{3\alpha-2}u\log u+\frac{17}{3\alpha-2}u\log\log u\right) \tag{3.13}$$

for all large x.

Suppose finally z is in the range (2.6). Writing z as $\exp((\log x)^{\frac{2}{3}}(\log\log x)^{\beta})$, we have from (3.1) and (3.7) that

$$k\Lambda\log k \leqslant \tfrac{9}{13}(\log x)^{\frac{1}{3}}(\log\log x)^{4-4\beta}(\log\log\log x)^{-1} \leqslant 19u(\log u)^{4-3\beta}(\log\log u)^{-1}$$

for all large x. Hence from (3.9)–(3.11) we have for any integer N and all sufficiently large x that

$$R_{x,z}(N) \leqslant \exp(20u(\log u)^{4-3\beta}(\log\log u)^{-1}). \tag{3.14}$$

Let $R_{x,z} = \max_N R_{x,z}(N)$. We conclude from (3.12)–(3.14) that for sufficiently large x we have

$$R_{x,z} \leqslant \begin{cases} \exp(O(u)), & \text{if (2.2) holds,} \\ \exp\left(48\dfrac{3-4\alpha}{3\alpha-2}u\log u+\dfrac{17}{3\alpha-2}u\log\log u\right), & \text{if (2.4) holds,} \\ \exp(20u(\log u)^{4-3\beta}(\log\log u)^{-1}), & \text{if (2.6) holds.} \end{cases} \tag{3.15}$$

For w such that $x \leqslant w \leqslant x+\frac{1}{2}y$, let

$$S_{x,z,y}(w) = S(w) = \sum_{\substack{(m,n,r,l_1,\dots,l_k)\in\mathscr{S}(x,z)\\ mnrl_1\dots l_k\in(w,w+y/2]}} \Lambda(r).$$

Note that $\Lambda(r) \leqslant \log r \leqslant \log z \leqslant \mathrm{e}^u$. Thus

$$\psi(x+y,z)-\psi(x,z) \geqslant \psi(w+\tfrac{1}{2}y,z)-\psi(w,z) \geqslant \mathrm{e}^{-u}R_{x,z}^{-1}S(w). \tag{3.16}$$

We shall show in the next section that

$$\max_{x\leqslant w\leqslant x+y/2} S(w) \geqslant y\cdot\exp(-(u+3k)(\log u+\log\log u+O(1))). \tag{3.17}$$

Using that $k=1$ in the range (2.2), $k \ll u/\log u$ in the range (2.4), and, for all large x, $k < \frac{1}{4}u$ in the range (2.6) (cf. (3.4)), Theorem 2.1 will follow from (3.15)–(3.17).

4. An analytic conclusion

In this section we conclude the proof of Theorem 2.1 and give a proof of Theorem 1.3.

As we saw in §3, Theorem 2.1 follows from (3.17). To show (3.17), it is sufficient to show that

$$\int_x^{x+y/2} S(w)\,\mathrm{d}w \geqslant y^2\cdot\exp(-(u+3k)(\log u+\log\log u+O(1))). \tag{4.1}$$

For both w and $w+\frac{1}{2}y$ not integers, we have

$$S(w) = \frac{-1}{2\pi\mathrm{i}}\int_{2-\mathrm{i}\infty}^{2+\mathrm{i}\infty}\frac{\zeta'}{\zeta}(s)\,\mathscr{M}(s)^2\,\mathscr{L}(s)^k\,\frac{(w+\frac{1}{2}y)^s-w^s}{s}\,\mathrm{d}s.$$

This is the Perron formula and it corresponds to display (2.9) in Harman (1991). Let

$$A(s) = \int_x^{x+y/2} \frac{(w+\frac{1}{2}y)^s - w^s}{s}\,\mathrm{d}w = \frac{(x+y)^{s+1} - 2(x+\frac{1}{2}y)^{s+1} + x^{s+1}}{s(s+1)}.$$

Thus interchanging the order of integration, we have

$$\int_x^{x+y/2} S(w)\,\mathrm{d}w = \frac{-1}{2\pi\mathrm{i}} \int_{2-\mathrm{i}\infty}^{2+\mathrm{i}\infty} \frac{\zeta'}{\zeta}(s)\,\mathscr{M}(s)^2\,\mathscr{L}(s)^k A(s)\,\mathrm{d}s. \tag{4.2}$$

We now move the path of integration to the curve $\mathscr{C} = \mathscr{C}_1 \cup \mathscr{C}_2 \cup \mathscr{C}_3 \cup \mathscr{C}_4 \cup \mathscr{C}_5$, where

$$\begin{aligned}
\mathscr{C}_1 &= \{s\colon s = 1+\mathrm{i}t, |t| \geqslant x\},\\
\mathscr{C}_2 &= \{s\colon s = 1+\mathrm{i}t, x/y \leqslant |t| \leqslant x\},\\
\mathscr{C}_3 &= \{s\colon s = 1+\mathrm{i}t, T \leqslant |t| \leqslant x/y\},\\
\mathscr{C}_4 &= \{s\colon s = \sigma+\mathrm{i}t, 1-a \leqslant \sigma \leqslant 1, |t| = T\},\\
\mathscr{C}_5 &= \{s\colon s = 1-a+\mathrm{i}t, |t| \leqslant T\},
\end{aligned}$$

and where $T = \exp(\frac{1}{6}c_6(\log z)^3/(\log x)^2)$, $a = 1/\log T$. We take the orientation of the curve $\mathscr{C}$ to be upwards. If x is sufficiently large the only singularity of the integrand in (4.2) encountered when moving the path of integration to $\mathscr{C}$ is the simple pole of $-\zeta'/\zeta$ at $s = 1$ with residue 1. This follows from the zero-free region $1-1/\log|t| \leqslant \sigma$ of $\zeta(s)$ for $|t|$ sufficiently large. We thus have from (4.2) that

$$\int_x^{x+y/2} S(w)\,\mathrm{d}w = \mathscr{M}(1)^2\,\mathscr{L}(1)^k A(1) + \frac{1}{2\pi\mathrm{i}} \int_{\mathscr{C}} \frac{\zeta'}{\zeta}(s)\,\mathscr{M}(s)^2\,\mathscr{L}(s)^k A(s)\,\mathrm{d}s. \tag{4.3}$$

We now estimate the main term in (4.3). First note that $A(1) = \frac{1}{4}y^2$. Next note that $\mathscr{L}(1)$ is at least the sum of the reciprocals of the primes in the interval $(L, \mathrm{e}L]$, so that for large x we have $\mathscr{L}(1) \geqslant 1/(2\log L) = 1/\log z$. Thus

$$\mathscr{L}(1)^k \geqslant (\log z)^{-k} = \exp(-k\alpha \log\log x) = \exp(-(\alpha/(1-\alpha))\,k\log u).$$

Using $\alpha \leqslant 1 - \log\log\log x/\log\log x$ and $k = 1$ in the range (2.2), we have

$$\mathscr{L}(1)^k \geqslant \begin{cases} \exp(-2u), & \text{if (2.2) holds,}\\ \exp(-4k\log u), & \text{if (2.4) or (2.6) holds.}\end{cases}$$

Thus from (3.5) we have

$$\mathscr{M}(1)^2\,\mathscr{L}(1)^k A(1) \geqslant y^2 \cdot \exp(-(u+3k)(\log u + \log\log u + O(1))).$$

Hence to show (4.1) and ultimately Theorem 2.1, it shall be sufficient to show, in light of (3.4), that

$$\int_{\mathscr{C}} \frac{\zeta'}{\zeta}(s)\,\mathscr{M}(s)^2\,\mathscr{L}(s)^k A(s)\,\mathrm{d}s \ll y^2 \exp(-2u\log u). \tag{4.4}$$

To show this we shall use Lemmas 2.8, 2.9 and 2.10 as well as

$$(\zeta'/\zeta)(s) \ll \log(|t|+2) \quad \text{on} \quad \mathscr{C}, \tag{4.5}$$

$$A(s) \ll \begin{cases} y^2 x^{\sigma-1}, & |t| \leqslant x/y\\ x^{1+\sigma}|t|^{-2}, & |t| > x/y\end{cases} \tag{4.6}$$

which correspond to (5.13) and (5.11) in Harman (1991).

For $i = 1, 2, 3, 4, 5$, let

$$E_i = \int_{\mathscr{C}_i} \frac{\zeta'}{\zeta}(s)\, \mathscr{M}(s)^2\, \mathscr{L}(s)^k A(s)\, \mathrm{d}s.$$

If we show each $E_i \ll y^2 \exp(-2u \log u)$, we will have (4.4) and the theorem.

The integral on $\mathscr{C}_1$. We use the trivial estimates $\mathscr{L}(s) \ll 1$, $\mathscr{M}(s) \ll 1$ on $\mathscr{C}_1$ as well as (4.5), (4.6) obtaining

$$E_1 \ll \int_x^\infty \frac{x^2 \log t}{t^2}\,\mathrm{d}t \ll x \log x = y^2 L^{-k-1} \log x$$

from (3.2). Thus $E_1 \ll y^2 \exp(-2u \log u)$.

The integral on $\mathscr{C}_2$. From (4.5) and (4.6) we have

$$E_2 \ll \int_{x/y}^x |\mathscr{M}(1+\mathrm{i}t)|^2 |\mathscr{L}(1+\mathrm{i}t)|^k \frac{x^2 \log t}{t^2}\,\mathrm{d}t$$

$$\ll x^2 \log x \max_{x/y \leqslant t \leqslant x} |\mathscr{L}(1+\mathrm{i}t)|^k \int_{x/y}^x |\mathscr{M}(1+\mathrm{i}t)|^2 \frac{1}{t^2}\,\mathrm{d}t.$$

From Lemma 2.9 and integration by parts we have

$$\int_{x/y}^x |\mathscr{M}(1+\mathrm{i}t)|^2 \frac{1}{t^2}\,\mathrm{d}t \ll (M+x)\Big(\sum_{m \in \mathscr{M}} \frac{1}{m^2}\Big)\frac{1}{x^2} + \int_{x/y}^x (M+t)\Big(\sum_{m\in\mathscr{M}} \frac{1}{m^2}\Big)\frac{1}{t^3}\,\mathrm{d}t$$

$$\ll \frac{1}{x/y} \sum_{m \in \mathscr{M}} \frac{1}{m^2} \ll \frac{y}{xM} = \frac{y^2}{x^2},$$

using (3.2) for the last step. If (2.2) holds, Lemma 2.8 implies that

$$\max_{x/y \leqslant t \leqslant x} |\mathscr{L}(1+\mathrm{i}t)| \ll \exp(-c_6 (\log L)^3/(\log x)^2) = \exp(-\tfrac{1}{8} c_6 (\log z)/u^2),$$

while if (2.4) or (2.6) holds, Lemma 2.10 and (3.6), (3.7) imply that

$$\max_{x/y \leqslant t \leqslant x} |\mathscr{L}(1+\mathrm{i}t)| \ll \exp(-\tfrac{1}{10} c_6 \cdot (\log z)/u^2) \log\log x.$$

Thus in every case we have

$$E_2 \leqslant y^2 \log x \exp(-\tfrac{1}{10} k\, c_6 (\log z)/u^2 + O(k \log\log\log x)),$$

where k is given by (3.1). Thus $E_2 \ll y^2 \exp(-2u \log u)$.

The integral on $\mathscr{C}_3$. From (4.5) and (4.6) we have

$$E_3 \ll y^2 \log x \max_{T \leqslant t \leqslant x/y} |\mathscr{L}(1+\mathrm{i}t)|^k \int_T^{x/y} |\mathscr{M}(1+\mathrm{i}t)|^2\,\mathrm{d}t.$$

From Lemma 2.9 and (3.2) we have

$$\int_T^{x/y} |\mathscr{M}(1+\mathrm{i}t)|^2\,\mathrm{d}t \ll \frac{x}{y} \sum_{m \in \mathscr{M}} \frac{1}{m^2} \ll \frac{x}{yM} = 1.$$

From Lemmas 2.8 and 2.10 we have

$$\max_{T\leqslant t\leqslant x/y} |\mathscr{L}(1+\mathrm{i}t)| \ll T^{-1}\log\log x = \exp\left(-\tfrac{1}{6}c_6(\log z)/u^2\right)\log\log x,$$

so that as with E_2 we get $E_3 \ll y^2\exp(-2u\log u)$.

The integral on $\mathscr{C}_4$. We use Lemmas 2.8 and 2.10 to get that

$$\mathscr{L}(\sigma+\mathrm{i}T) \ll L^{1-\sigma}T^{-1}\log\log T = L^{1-\sigma}\exp\left(-\tfrac{1}{6}c_6(\log z)/u^2\right)\log\log T$$

for σ such that $1-1/\log T = 1-a \leqslant \sigma \leqslant 1$. We also use the trivial estimate $|\mathscr{M}(\sigma+\mathrm{i}T)| \ll M^{1-\sigma}$. Thus from (4.5) and (4.6) we have

$$E_4 \leqslant y^2\log T\exp\left(-\tfrac{1}{6}kc_6(\log z)/u^2 + O(k\log\log\log x)\right)\int_{1-a}^{1} L^{k(1-\sigma)}M^{2(1-\sigma)}x^{\sigma-1}\,\mathrm{d}\sigma.$$

By (3.1) we have

$$\log T\int_{1-a}^{1} L^{k(1-\sigma)}M^{2(1-\sigma)}x^{\sigma-1}\,\mathrm{d}\sigma = \frac{1}{a}\int_{1-a}^{1} L^{\sigma-1}\,\mathrm{d}\sigma \leqslant 1,$$

so that $E_4 \ll y^2\exp(-2u\log u)$.

The integral on $\mathscr{C}_5$. From Lemmas 2.8 and 2.10 we have

$$|\mathscr{L}(1-a+\mathrm{i}t)| \ll \frac{L^a}{1+|t|}\log\log L$$

on $\mathscr{C}_5$. Using the trivial estimate $|\mathscr{M}(1-a+\mathrm{i}t)| \ll M^a$ and (4.5), (4.6), (3.1), we have

$$\begin{aligned} E_5 &\leqslant y^2x^{-a}L^{ka}M^{2a}\log T(\log\log x)^k\,\mathrm{e}^{O(k)}\int_0^T (1+t)^{-k}\,\mathrm{d}t \\ &\leqslant y^2L^{-a}(\log T)^2(\log\log x)^k\,\mathrm{e}^{O(k)} \ll y^2\exp(-2u\log u). \end{aligned}$$

This completes the proof of Theorem 2.1. □

Remark. S. W. Graham has pointed out to us that using the methods on pp. 62 and 63 of Titchmarsh (1986) one may obtain an estimate for $\mathscr{P}(s) = \Sigma_{L<p\leqslant \mathrm{e}L} p^{-s}$, where p runs over primes, of the same general flavour as Lemma 2.8, though a little weaker. Suppose we were to substitute $\mathscr{P}(s)$ for $\mathscr{L}(s)$ in the proof of Theorem 2.1. We then would not need Lemma 2.10 and the estimate for $R_{x,z}$ would be much simpler. Further, for a large part of the range (2.4) we would obtain an estimate of the same quality as (2.3). However, the estimate for $\mathscr{P}(s)$ is sufficiently weaker than the one for $\mathscr{L}(s)$ that we would not be able to prove anything about the range (2.6), which is the only range we actually apply in the analysis of our algorithm.

Proof of Theorem 1.3. The result follows easily from Theorem 2.1, from the choice of c_1 given in the proof of the Theorem, and from the remark following Lemma 2.8 concerning the choice of c_6. □

We thank S. W. Graham for his critical comments of an earlier draft of this paper. In addition we thank the National Science Foundation for partial support under (respectively) grant numbers DMS 9002939, DMS 9104316, DMS 9002538. J.P. is grateful to MSRI (Berkeley) for hospitality and support.

References

Adleman, L. M. & Huang, M.-D. 1987 Recognizing primes in random polynomial time. In *Proc. 19th ACM Symp. Theory Comput.*, pp. 462–469. New York: Association for Computing Machinery.

Adleman, L. M. & Huang, M.-D. 1992 *Primality testing and abelian varieties over finite fields*. Lecture Notes in Mathematics, vol. 1512. Berlin: Springer-Verlag.

Balog, A. 1987 On the distribution of integers having no large prime factors. *Astérisque* **147–148**, 27–31.

Canfield, E. R., Erdös, P. & Pomerance, C. 1983 On a problem of Oppenheim concerning 'factorisatio numerorum'. *J. Number Theory* **17**, 1–28.

Friedlander, J. B. 1976 Integers free from large and small primes. *Proc. Lond. math. Soc.* **33**, 565–576.

Goldwasser, S. & Kilian, J. 1986 Almost all primes can be quickly certified. In *Proc. 18th ACM Symp. Theory Comp.*, pp. 316–329. New York: Association for Computing Machinery.

Harman, G. 1991 Short intervals containing numbers without large prime factors. *Math. Proc. Camb. phil. Soc.* **109**, 1–5.

Lenstra, A. K. & Lenstra, H. W., Jr 1990 Algorithms in number theory. In *Handbook of theoretical computer science* (ed. J. van Leeuwen), vol. A (*Algorithms and complexity*), pp. 674–714. Amsterdam: Elsevier.

Lenstra, H. W., Jr 1987 Factoring integers with elliptic curves. *Ann. Math.* **126**, 649–673.

Lenstra, H. W., Jr & Pomerance, C. 1992 A rigorous time bound for factoring integers. *J. Am. math. Soc.* **5**, 483–516.

Montgomery, H. L. 1971 *Topics in multiplicative number theory*. Lecture Notes in Mathematics, vol. 227. Berlin: Springer-Verlag.

Pollard, J. M. 1974 Theorems on factorization and primality testing. *Proc. Camb. phil. Soc.* **76**, 521–528.

Pomerance, C. 1982 Analysis and comparison of some integer factoring algorithms. In *Computational methods in number theory* (ed. H. W. Lenstra, Jr & R. Tijdeman), pp. 89–139. Math. Centre Tracts 154/155. Amsterdam: Mathematisch Centrum.

Pomerance, C. 1987 Fast, rigorous factorization and discrete logarithm algorithms. In *Discrete algorithms and complexity* (ed. D. S. Johnson, T. Nishizeki, A. Nozaki & H. S. Wilf), pp. 119–143. Orlando: Academic Press.

Saias, E. 1992 Entiers sans grand ni petit facteur premier. I. *Acta Arith.* **61**, 347–374.

Saias, E. 1993 Entiers sans grand ni petit facteur premier. II. *Acta Arith.* (In the press.)

Strassen, V. 1977 Einige Resultate über Berechnungskomplexität. *Jahresber. Deutsch. Math.-Verein.* **78**, 1–8.

Titchmarsh, E. C. 1986 *The theory of the Riemann zeta-function*, 2nd edn (revised by D. R. Heath-Brown). Oxford: Clarendon Press.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES