Research Article

Francesco Sica*

Factoring with Hints

https://doi.org/10.1515/jmc-2020-0078
Received Jun 05, 2019; accepted Jul 01, 2019

Abstract: We introduce a new approach to (deterministic) integer factorisation, which could be described in the cryptographically fashionable term of "factoring with hints": we prove that, for any $\epsilon > 0$, given the knowledge of the factorisations of $O(N^{1/3+\epsilon})$ terms surrounding $N = pq$ product of two large primes, we can recover deterministically p and q in $O(N^{1/3+\epsilon})$ bit operations. This shows that the factorisations of close integers are non trivially related and that consequently one can expect more results along this line of thought.

Keywords: Riemann zeta function, factorisation of RSA moduli, complex analysis

2010 Mathematics Subject Classification: 11M06; 94A60

1 Introduction

The problem of quickly factoring large integers is central in cryptography and computational number theory. The current state of the art in factoring large integers N, the Number Field Sieve algorithm [5, 6], stems from the earlier Quadratic Sieve [11] and Continued Fraction [9]. We should also mention the Elliptic Curve Method by H. Lenstra [7], which is particularly useful when N has a small prime factor p. They are all probabilistic factoring algorithms.

These algorithms have *heuristic* running times respectively $O\big(e^{c(\log N)^{1/3}(\log\log N)^{2/3}}\big)$, $O\big(e^{c(\log N)^{1/2}(\log\log N)^{1/2}}\big)$ and $O\big(e^{c(\log p)^{1/2}(\log\log p)^{1/2}}\big)$, for some constant c (not always the same). The first two strive to find nontrivial arithmetical relations of the form $x^2 \equiv y^2 \pmod N$ (which lead to a nontrivial factor by computing $\gcd(N, x+y)$), whereas the third is a generalisation of Pollard's $p-1$ method [10], involving computations in some elliptic curve group instead of $\mathbb{Z}/N$. We should note, however, that there exist probabilistic algorithms with proved running time $O\big(\exp((1+o(1))(\log N)^{1/2}(\log\log N)^{1/2})\big)$ [8]. As far as the author is aware, no such rigorous bound exists in the form $O\big(\exp\big((\log N)^c\big)\big)$ for $c < 1/2$. Similarly, no deterministic subexponential algorithm is currently known, the best one being Shanks' square form factorization SQUFOF which runs in $O(N^{1/4+\epsilon})$, or in $O(N^{1/5+\epsilon})$ on the Extended Riemann Hypothesis. Recently Hittmeir [4] has somewhat improved Shanks' unconditional result to $O\big(N^{1/4}\exp(\frac{-C\log N}{\log\log N})\big)$ for some explicit constant $C > 0$. This is currently the best unconditional deterministic factoring algorithm.

In this work, we want to introduce a new paradigm in integer factorisation, one that doesn't supersede previous efforts, but rather complements it by showing that the factorisation of a small number of consecutive integers is related in a nontrivial way. Therefore, if numbers close to a product $N = pq$ of two primes are easier to factor than N itself, we can expect a reduction in the time to factor N. Here we content ourselves with a first nontrivial result.

Theorem 1. *Let $N = pq$ a product of two primes. Then, given an arbitrary $\epsilon > 0$, the factors p and q can be recovered in $O(N^{1/3+\epsilon})$ bit operations from the knowledge of the factorisations of $O(N^{1/3+\epsilon})$ integers closest to N. The memory requirement is polynomial for the computational part.*

***Corresponding Author: Francesco Sica:** School of Sciences and Humanities, Nazarbayev University, 53 Kabanbay Batyr, Nur-Sultan, Kazakhstan; Email: francesco.sica@nu.edu.kz

Remark that $O(N^{1/3+\epsilon})$ integers close to $N = pq$ do no contain the factors p or q in the case of a RSA modulus, when $p, q = O(\sqrt{N})$. The $O(N^{1/3+\epsilon})$ bit operations mentioned in the theorem essentially involve the factorisations of the first $O(N^{1/3+\epsilon})$ integers, where similarly the factors p, q of a RSA modulus would not appear. Thus we can loosely say that our result proves that the factorisation of $N = pq$ is related to the factorisations of the $O(N^{1/3+\epsilon})$ integers closest to it and to the $O(N^{1/3+\epsilon})$ smallest positive integers.

The structure of this article will be as follows. After recalling notations (Section 2) we explain the main idea of the method: finding a close enough approximation to the value of a multiplicative function $\sigma_{1/2}(N)$ and deduce a corresponding approximation a to p dividing N (Section 3).

In Section 4, we use generating functions (products of zeta functions) and their inverse Mellin transforms when multiplied by an appropriate kernel to define the quantities that we will be led to evaluate: $F_v(x)$ and $P_v(x)$.

In Section 6, we obtain a different expression for $F_v(x)$ by making use of the functional equation of the generating function. We discover that the new expression can be easily computed save for two families of oscillating series.

Finally, in Section 7, we show that by computing around $N^{1/3+\epsilon}$ terms in the oscillating series, each of which can be done in polynomial time, one can get a block approximation to $\sigma_{1/2}(n)$ for $n = N$ together with about $N^{1/3+\epsilon}$ of its neighbours. Therefore, knowing the factorisation of these neighbours would allow us to find an approximation to $\sigma_{1/2}(N)$ and therefore to a divisor p of N.

2 Notations

In this work $N = pq$ where p, q are distinct prime numbers. We follow standard notations in analytic number theory and indeed a classical reference on the subject is the treatise of Davenport [3]. In particular, we will make liberal use of the O notation in Landau's as well as Vinogradov's form ($\ll$). Hence, for instance

$$f(u) = O\big(g(u)\big) \iff f(u) \ll g(u)$$

means that $g(u) > 0$ and $|f(u)|/g(u)$ is bounded above (usually as $u \to \infty$ or $u \to 0^+$, depending clearly on the context). Unless specified, the implied constants are absolute.

Any sum such as

$$\sum_{abc=n} a^2 bc$$

is to be understood as taken over all positive integers a, b, c such that $abc = n$. We also define

$$\sum_{a|n} f(a) = \sum_{ab=n} f(a)$$

so that for instance the number of divisors of n is $\sum_{d|n} 1$ and its sum of divisors $\sum_{d|n} d$. We also write $s = \sigma + it$, with $\sigma, t \in \mathbb{R}$, according to the established convention in analytic number theory.

Finally, we write $a \doteq b$ to signify that $a = b +$ terms that are not necessarily negligible in size but can be computed in polynomial time (in the bit size of the challenge to be factored), so that they are negligible in time.

3 Choice of a Multiplicative Function

For $\lambda \in \mathbb{R}$ define

$$\sigma_\lambda(n) = \sum_{d|n} d^\lambda \quad .$$

Our goal will be to compute $\sigma_{1/2}(N) = 1+\sqrt{N}+\sqrt{p}+\frac{\sqrt{N}}{\sqrt{p}}$ within $O(1/N)$. If so, then one gets an approximation $\mathcal{A}$ to

$$f(p) = \sqrt{p} + \frac{\sqrt{N}}{\sqrt{p}} = \mathcal{A} + O\left(\frac{1}{N}\right) \quad . \tag{1}$$

Let us study the function in $(0, \infty)$

$$f(z) = \sqrt{z} + \frac{\sqrt{N}}{\sqrt{z}} \Rightarrow f'(z) = \frac{1}{2\sqrt{z}}\left(1 - \frac{\sqrt{N}}{z}\right) \Rightarrow f''(z) = \frac{1}{4z^{3/2}}\left(\frac{3\sqrt{N}}{z} - 1\right) \quad .$$

The function f is convex in $(0, 3\sqrt{N})$ with a unique critical point (and therefore absolute minimum) at $z = \sqrt{N}$. We will suppose that $N = pq$ with $p < \sqrt{N} < q$. In fact, we may as well suppose that $p \le \sqrt{N} - 2$ by inspection. Note that $f''(z) \ge N^{-3/4}/2$ for $z \le \sqrt{N}$ and therefore $|f'(z)| \ge N^{-3/4}/2$ for $z \le \sqrt{N} - 1$. Define $a \in (0, \sqrt{N} - 1]$ by $f(a) = \mathcal{A}$. To see that such a exists, notice that f is decreasing in $(0, \sqrt{N}]$. If $\mathcal{A} < f(\sqrt{N} - 1)$, then, for some $\theta \in (\sqrt{N} - 2, \sqrt{N} - 1)$, we can write

$$\left|\mathcal{A} - f(p)\right| < |f(\sqrt{N} - 1) - f(\sqrt{N} - 2)| = |f'(\theta)| \ge \frac{1}{2N^{3/4}} \quad ,$$

contradicting (1). Given then $a \in (0, \sqrt{N} - 1]$ with $f(a) = \mathcal{A}$, we obtain, for some $\xi \le \sqrt{N} - 1$,

$$|a - p|\ \left|f'(\xi)\right| = \left|f(a) - f(p)\right| = \left|\mathcal{A} - f(p)\right| \ll \frac{1}{N} \Rightarrow p = a + O\left(\frac{1}{N^{1/4}}\right)$$

and therefore $p = \lfloor a \rceil$, the integer nearest to a.

4 Choice of a Test Function

Consider the Riemann zeta function

$$\zeta(s) = \sum_{n \ge 1} \frac{1}{n^s} \quad ,$$

convergent for $\Re s > 1$. Then

$$\zeta(s)\zeta(s - 1/2) = \sum_{n=1}^{\infty} \frac{\sigma_{1/2}(n)}{n^s} \quad ,$$

absolutely convergent whenever $\Re s > 3/2$. Now let for $\nu \in \mathbb{N}$[1] with $\nu \ge 2$,

$$f(t) = \begin{cases} (1-t)^{\nu-1} & 0 \le t \le 1, \\ 0 & t \ge 1. \end{cases}$$

The Mellin transform of f is by definition the beta function

$$B(\nu, s) = \frac{\Gamma(\nu)\Gamma(s)}{\Gamma(s+\nu)} = \int_0^{\infty} f(t)t^{s-1}\, dt$$

hence by the inverse Mellin transform[2],

$$\frac{1}{2\pi i}\int_{5/2-i\infty}^{5/2+i\infty} \zeta(s)\zeta(s - 1/2)\,\frac{\Gamma(\nu)\Gamma(s)}{\Gamma(s+\nu)}x^s\, ds = \sum_{n \le x} \sigma_{1/2}(n) f\left(\frac{n}{x}\right). \tag{2}$$

1 In fact, ν doesn't need to be an integer, but it simplifies calculations to assume so.

2 We will also use the notation $\int_{(c)}$ instead of $\int_{c-i\infty}^{c+i\infty}$.

Call the right-hand side

$$F_\nu(x) = \sum_{n\le x} \sigma_{1/2}(n) f\left(\frac{n}{x}\right) = \sum_{n\le x} \sigma_{1/2}(n) \left(1-\frac{n}{x}\right)^{\nu-1}$$

and note that

$$P_\nu(x) = x^{\nu-1} F_\nu(x) = \sum_{n\le x} \sigma_{1/2}(n)(x-n)^{\nu-1}$$

is a piecewise polynomial (given by a different expression between consecutive integers).

5 Functional Equation of the Riemann Zeta Function

The Riemann zeta function is a meromorphic function having a simple pole with residue 1 at $s = 1$ and satisfying the functional equation (given here in asymmetric form)

$$\zeta(s) = \frac{1}{2\pi i}(2\pi)^s\ \Gamma(1-s)\zeta(1-s)\left(e^{i\pi s/2} - e^{-i\pi s/2}\right) = \frac{1}{\pi}(2\pi)^s\ \Gamma(1-s)\zeta(1-s)\sin\frac{\pi s}{2}\ .$$

6 Another Expression for $F_\nu(x)$

A standard "integration line moving"[3] (to $\Re s = -1/4$) argument in the integral of (2) will get us to the following, after picking up the residues of the integrand at $s = 3/2$, $s = 1$ and $s = 0$,

$$F_\nu(x) = \zeta(3/2)\frac{\Gamma(\nu)\Gamma(3/2)}{\Gamma(\nu+3/2)}x^{3/2} + \frac{\zeta(1/2)}{\nu}x + \zeta(0)\zeta(-1/2) + \frac{1}{2\pi i}\int\limits_{(-1/4)} \zeta(s)\zeta(s-1/2)\frac{\Gamma(\nu)\Gamma(s)}{\Gamma(s+\nu)}x^s\,ds\ .$$

In fact, we can move the line of integration to $\Re s = -1/4$, since to the right of that line, for any given $\epsilon > 0$,

$$|\zeta(s)\zeta(s-1/2)| \ll |t|^{2+\epsilon}\ ,$$

while

$$\left|\frac{\Gamma(s)}{\Gamma(s+\nu)}\right| \ll |t|^{-\nu}\ .$$

In particular the integral on the right-hand side is absolutely convergent when $\nu \ge 4$. It is this integral is the next focus of our investigation. It is natural at this point to use the functional equation. We get quite straightforwardly

$$\begin{aligned}
&\frac{1}{2\pi i}\int\limits_{(-1/4)} \zeta(s)\zeta(s-1/2)\frac{\Gamma(\nu)\Gamma(s)}{\Gamma(s+\nu)}x^s\,ds = \frac{1}{(2\pi i)^3}\int\limits_{(-1/4)} (2\pi)^s\,\Gamma(1-s)\zeta(1-s)\sin\frac{\pi s}{2}\\
&\times(2\pi)^{s-1/2}\,\Gamma(3/2-s)\zeta(3/2-s)\sin\left(\frac{\pi s}{2}-\frac{\pi}{4}\right)\frac{\Gamma(\nu)\Gamma(s)}{\Gamma(s+\nu)}x^s\,ds = \frac{e^{-i\pi/4}}{(2\pi i)^3\sqrt{2\pi}}\\
&\times\int\limits_{(-1/4)} (4\pi^2 x)^s e^{i\pi s}\Gamma(1-s)\zeta(1-s)\Gamma\left(\frac{3}{2}-s\right)\zeta\left(\frac{3}{2}-s\right)\frac{\Gamma(\nu)\Gamma(s)}{\Gamma(s+\nu)}\,ds + \frac{e^{i\pi/4}}{(2\pi i)^3\sqrt{2\pi}}
\end{aligned}$$

3 This is done by applying Cauchy's residue theorem to a rectangle whose long sides rest on $\Re s = 5/2$ and $\Re s = -1/4$ and letting the short sides tend to infinity, where their contribution to the contour integral becomes zero, as justified in the subsequent lines.

$$\times \int_{(-1/4)} (4\pi^2 x)^s e^{-i\pi s}\Gamma(1-s)\zeta(1-s)\Gamma\left(\frac{3}{2}-s\right)\zeta\left(\frac{3}{2}-s\right)\frac{\Gamma(v)\Gamma(s)}{\Gamma(s+v)}\,ds$$
$$-\frac{1}{(2\pi i)^3\sqrt{\pi}}\int_{(-1/4)} (4\pi^2 x)^s\Gamma(1-s)\zeta(1-s)\Gamma(3/2-s)\zeta(3/2-s)\frac{\Gamma(v)\Gamma(s)}{\Gamma(s+v)}\,ds$$
$$=\frac{e^{-i\pi/4}x}{2\pi i\sqrt{2\pi}}\int_{(5/4)} (4\pi^2 x)^{-s}e^{-i\pi s}\Gamma(s)\zeta(s)\Gamma(s+1/2)\zeta(s+1/2)\frac{\Gamma(v)\Gamma(1-s)}{\Gamma(1-s+v)}\,ds$$
$$+\frac{e^{i\pi/4}x}{2\pi i\sqrt{2\pi}}\int_{(5/4)} (4\pi^2 x)^{-s}e^{i\pi s}\Gamma(s)\zeta(s)\Gamma(s+1/2)\zeta(s+1/2)\frac{\Gamma(v)\Gamma(1-s)}{\Gamma(1-s+v)}\,ds$$
$$+\frac{x}{2\pi i\sqrt{\pi}}\int_{(5/4)} (4\pi^2 x)^{-s}\Gamma(s)\zeta(s)\Gamma(s+1/2)\zeta(s+1/2)\frac{\Gamma(v)\Gamma(1-s)}{\Gamma(1-s+v)}\,ds\ .$$

Using the Legendre duplication formula

$$\Gamma(s)\Gamma\left(s+\frac{1}{2}\right)=\sqrt{\pi}\,2^{1-2s}\Gamma(2s)\ ,$$

together with the functional equations $s\Gamma(s)=\Gamma(s+1)$ and $\Gamma(s)\Gamma(1-s)=\pi\csc\pi s$, we obtain

$$\Gamma\left(s+\frac{1}{2}\right)\frac{\Gamma(s)\Gamma(1-s)}{\Gamma(1-s+v)}=\Gamma\left(s+\frac{1}{2}\right)\Gamma(s-v)(\cos\pi v-\sin\pi v\cot\pi s)=(-1)^v\frac{\sqrt{\pi}\,2^{1-2s}\Gamma(2s)}{(s-1)(s-2)\cdots(s-v)}\ . \quad (3)$$

We can further transform (3) by noting that there exist unique constants $c_{0,v}=1,\dots,c_{v,v}$ such that

$$\frac{1}{(s-1)(s-2)\cdots(s-v)}=\frac{2^v}{(2s-2)(2s-4)\cdots(2s-2v)}$$
$$=\frac{2^v c_{0,v}}{(2s-1)(2s-2)\cdots(2s-v)}+\frac{2^v c_{1,v}}{(2s-1)(2s-2)\cdots(2s-(v+1))}+\cdots$$
$$+\frac{2^v c_{v,v}}{(2s-1)(2s-2)\cdots(2s-2v)}$$

whenever this expression makes sense. To see this, multiply both sides by $(2s-1)(2s-2)\cdots(2s-2v)$. The resulting left-hand side is a polynomial of degree v, expressed as a linear combination of the polynomials resulting from the right-hand side, which form a basis of the vector space of polynomials of degree $\le v$. For instance, $c_{0,1}=c_{1,1}=1$ and $c_{0,4}=1$, $c_{1,4}=10$, $c_{2,4}=45$, $c_{3,4}=c_{4,4}=105$. From (3) we get

$$(-1)^v\Gamma\left(s+\frac{1}{2}\right)\Gamma(s-v)=(-1)^v\sqrt{\pi}\,2^{v+1-2s}\sum_{m=0}^{v}c_{m,v}\Gamma(2s-v-m)\ .$$

Putting it together we obtain

$$\frac{1}{2\pi i}\int_{(-1/4)}\zeta(s)\zeta(s-1/2)\frac{\Gamma(v)\Gamma(s)}{\Gamma(s+v)}x^s\,ds=(-1)^v 2^{v+1/2}e^{-i\pi/4}x\Gamma(v)\sum_{m=0}^{v}c_{m,v}\sum_{n\ge1}\sigma_{-1/2}(n)$$
$$\times\frac{1}{2\pi i}\int_{(5/4)}(16\pi^2 xn)^{-s}e^{-i\pi s}\Gamma(2s-v-m)\,ds+(-1)^v 2^{v+1/2}e^{i\pi/4}x\Gamma(v)\sum_{m=0}^{v}c_{m,v}\sum_{n\ge1}\sigma_{-1/2}(n)$$
$$\times\frac{1}{2\pi i}\int_{(5/4)}(16\pi^2 xn)^{-s}e^{i\pi s}\Gamma(2s-v-m)\,ds$$
$$+(-1)^v 2^{v+1}x\Gamma(v)\sum_{m=0}^{v}c_{m,v}\sum_{n\ge1}\sigma_{-1/2}(n)\frac{1}{2\pi i}\int_{(5/4)}(16\pi^2 xn)^{-s}\Gamma(2s-v-m)\,ds\ .$$

We have, for $y > 0$,

$$\frac{1}{2\pi i}\int_{(1/2)} y^{-s}\Gamma(s)\,ds = e^{-y}$$

and after collecting the residues of the gamma function at the negative integers,

$$\frac{1}{2\pi i}\int_{(-(2k+1)/2)} y^{-s}\Gamma(s)\,ds = e^{-y} - \left(1 - y + \frac{y^2}{2!} + \cdots + (-1)^k\frac{y^k}{k!}\right) \qquad k \geq 0\ .$$

Remark that if $k \geq 1$, since $|\Gamma(s)| < e^{-\pi|t|/2}|t|^{-k-1}$ on $\Re s = -k-1/2$, the left-hand side of the previous expression is analytic for $\Re y > 0$ and continuous up to $\Re y = 0$. Therefore the previous formula for $k \geq 1$ holds in the closed half-plane $\Re y \geq 0$. With this explicit expression we find that

$$\begin{aligned}
&\frac{1}{2\pi i}\int_{(-1/4)} \zeta(s)\zeta(s-1/2)\,\frac{\Gamma(v)\Gamma(s)}{\Gamma(s+v)}x^s\,ds = (-1)^v 2^{v+1/2}e^{-i\pi/4}x\Gamma(v)\sum_{m=0}^{v} c_{m,v}\sum_{n\geq 1}\sigma_{-1/2}(n)\\
&\times\frac{1}{2\pi i}\int_{(5/4)} (16\pi^2 xn)^{-s}e^{-i\pi s}\Gamma(2s-v-m)\,ds + (-1)^v 2^{v+1/2}e^{i\pi/4}x\Gamma(v)\sum_{m=0}^{v} c_{m,v}\sum_{n\geq 1}\sigma_{-1/2}(n)\\
&\times\frac{1}{2\pi i}\int_{(5/4)} (16\pi^2 xn)^{-s}e^{i\pi s}\Gamma(2s-v-m)\,ds\\
&+(-1)^v 2^{v+1}x\Gamma(v)\sum_{m=0}^{v} c_{m,v}\sum_{n\geq 1}\sigma_{-1/2}(n)\frac{1}{2\pi i}\int_{(5/4)} (16\pi^2 xn)^{-s}\Gamma(2s-v-m)\,ds\\
&=(-1)^v 2^{v+1/2}e^{-i\pi/4}x\Gamma(v)\sum_{m=0}^{v}\frac{c_{m,v}}{2(4\pi i)^{v+m}x^{v/2+m/2}}\sum_{n\geq 1}\sigma_{-1/2}(n)\frac{e^{-4\pi i\sqrt{xn}}}{n^{v/2+m/2}} \qquad (4)\\
&-(-1)^v 2^{v-1/2}e^{-i\pi/4}x\Gamma(v)\times\sum_{m=0}^{v} c_{m,v}\sum_{k=0}^{v-1+m}\frac{(-1)^{v-3+m-k}}{(v-3+m-k)!(4\pi i)^{3+k}x^{3/2+k/2}}\sum_{n\geq 1}\frac{\sigma_{-1/2}(n)}{n^{3/2+k/2}}\\
&+(-1)^v 2^{v+1/2}e^{i\pi/4}x\Gamma(v)\sum_{m=0}^{v}\frac{(-1)^{v+m}c_{m,v}}{2(4\pi i)^{v+m}x^{v/2+m/2}}\sum_{n\geq 1}\sigma_{-1/2}(n)\frac{e^{4\pi i\sqrt{xn}}}{n^{v/2+m/2}} \qquad (5)\\
&-(-1)^v 2^{v-1/2}e^{i\pi/4}x\Gamma(v)\\
&\times\sum_{m=0}^{v} c_{m,v}\sum_{k=0}^{v-1+m}\frac{(-1)^{v+m}}{(v-3+m-k)!(4\pi i)^{3+k}x^{3/2+k/2}}\sum_{n\geq 1}\frac{\sigma_{-1/2}(n)}{n^{3/2+k/2}}\\
&+(-1)^v 2^{v+1}x\Gamma(v)\sum_{m=0}^{v}\frac{c_{m,v}}{2(4\pi)^{v+m}x^{v/2+m/2}}\sum_{n\geq 1}\sigma_{-1/2}(n)\frac{e^{-4\pi\sqrt{xn}}}{n^{v/2+m/2}}\\
&-(-1)^v 2^v x\Gamma(v)\sum_{m=0}^{v} c_{m,v}\sum_{k=0}^{v-1+m}\frac{(-1)^{v-3+m-k}}{(v-3+m-k)!(4\pi)^{3+k}x^{3/2+k/2}}\sum_{n\geq 1}\frac{\sigma_{-1/2}(n)}{n^{3/2+k/2}}\ .
\end{aligned}$$

In this last expression, the only terms that we cannot calculate explicitly are the two inner series in (4) and (5).

7 Factoring with Hints

We show here, given $0 < \epsilon < 1$, how to calculate in $O(N^{1/3+\epsilon})$ bit operations, assuming the factorisation knowledge of $O(N^{1/3+\epsilon})$ integers immediately around $N = pq$, the quantity $\sigma_{1/2}(N) = \sqrt{N} + 1 + \sqrt{p} + \sqrt{q}$ within $O(N^{-1})$, which is sufficient to derive p and q. In the following, we suppose that v is a fixed (in terms of N) integer with $v \geq 20/3\epsilon$. The work done in the previous section allows us to write

$$P_\nu(x) \doteq (-1)^\nu 2^{\nu-1/2} e^{-i\pi/4} x^{\nu/2} \Gamma(\nu) \sum_{m=0}^{\nu} \frac{c_{m,\nu}}{(4\pi i)^{\nu+m} x^{m/2}} \sum_{n\geq 1} \sigma_{-1/2}(n) \frac{e^{-4\pi i\sqrt{xn}}}{n^{\nu/2+m/2}} \tag{6}$$

$$+(-1)^\nu 2^{\nu-1/2} e^{i\pi/4} x^{\nu/2} \Gamma(\nu) \sum_{m=0}^{\nu} \frac{(-1)^{\nu+m} c_{m,\nu}}{(4\pi i)^{\nu+m} x^{m/2}} \sum_{n\geq 1} \sigma_{-1/2}(n) \frac{e^{4\pi i\sqrt{xn}}}{n^{\nu/2+m/2}} \ . \tag{7}$$

In fact, the series without the oscillating exponential terms can be calculated in polynomial time to within $O(x^{-\nu})$ by methods of [1, 2] because

$$\sum_{n\geq 1} \frac{\sigma_{-1/2}(n)}{n^{3/2+k/2}} = \zeta\left(\frac{3}{2}+\frac{k}{2}\right)\zeta\left(2+\frac{k}{2}\right) \ .$$

Having fixed $\epsilon > 0$, we approximate the series

$$\sum_{n\geq 1} \sigma_{-1/2}(n) \frac{e^{\pm 4\pi i\sqrt{xn}}}{n^{\nu/2+m/2}}$$

by its $[x^{1/3+\epsilon/2}]$-th partial sum, with a corresponding error

$$\ll \sum_{n\geq x^{1/3+\epsilon/2}} \frac{\sigma_{-1/2}(n)}{n^{\nu/2}} \ll \sum_{n\geq x^{1/3+\epsilon/2}} \frac{1}{n^{\nu/2-1}} \ll x^{-(1/3+\epsilon/2)(\nu/2-2)}$$

and therefore (6) and (7) can be replaced by the corresponding expressions where the inner sums in n are truncated at $n \leq x^{1/3+\epsilon/2}$ with a total error

$$\ll x^{\nu/2} x^{-(1/3+\epsilon/2)(\nu/2-2)} \leq x^{\nu/3} \ ,$$

since $\epsilon\nu \geq 20/3$ (and $\epsilon < 1$). Remark that the truncated series with $y = x^{1/3+\epsilon/2}$

$$\sum_{n\leq y} \sigma_{-1/2}(n) \frac{e^{\pm 4\pi i\sqrt{xn}}}{n^{\nu/2+m/2}} = \sum_{n_1 n_2 \leq y} \frac{e^{\pm 4\pi i\sqrt{xn_1n_2}}}{n_1^{\nu/2+m/2} n_2^{\nu/2+(m+1)/2}} \tag{8}$$

can be computed trivially within $O(x^{-\nu})$ in $O(x^{1/3+\epsilon})$ bit operations since there are $O(y \log y)$ positive integer pairs (n_1, n_2) with $n_1 n_2 \leq y$. Computing each term in the sum to the required precision can be achieved by calculating

$$\exp(4\pi i\sqrt{xn_1n_2})$$

to within $O(x^{-\nu})$. This can be done by calculating $a \in [0, 2\pi)$ such that $a \equiv \sqrt{xn_1n_2} \pmod 1$ with error $\ll x^{-\nu}$ and then using a Maclaurin expansion of the exponential truncated after $\nu \log x$ terms. To summarise, we can compute the right-hand side of (6), (7) within $O(x^{\nu/3})$ in $O(x^{1/3+\epsilon})$ bit operations.

On the other hand, let $h > 0$ and define $\nabla_h P_\nu(x) (= \nabla_h^1 P_\nu(x)) = P_\nu(x) - P_\nu(x-h)$ and $\nabla_h^{k+1} P_\nu(x) = \nabla_h \nabla_h^k P_\nu(x)$ for $k \geq 1$. The following statements can easily be shown by induction.

1. If P is a polynomial of degree d then $\nabla_h^{d+1} P = 0$,
2. $\nabla_h^k P_\nu(x) = \sum_{i=0}^k \binom{k}{i} P_\nu(x-ih)$.

Letting $x = N + N^{1/3+\epsilon}$ and $h = N^{1/3+\epsilon}$ we see that $\nabla_h^\nu P_\nu(x)$ can be expressed as

$$\sigma_{1/2}(N) N^{(\nu-1)(1/3+\epsilon)} + \text{ terms involving only } \sigma_{1/2}(n) \text{ for } x - \nu N^{1/3+\epsilon} \leq n \leq x,$$

with $n \neq N$. Using (6), (7) again and our discussion on the right-hand side of this equation, we see that $\nabla_h^\nu P_\nu(x)$ can also be computed within $O(x^{\nu/3})$ with $O(x^{1/3+\epsilon})$ bit operations.

Therefore we can compute in $O(N^{1/3+\epsilon})$ bit operations an approximation of $N^{(\nu-1)(1/3+\epsilon)} \sigma_{1/2}(N)$ within $O(N^{\nu/3})$. This leads to an approximation of $\sigma_{1/2}(N)$ within

$$N^{\nu/3-(\nu-1)(1/3+\epsilon)} \ll N^{-1}$$

since $\epsilon\nu \geq 7/3$. Recovering $p \mid N$ is explained in Section 3.

8 Final Considerations

Our method relates the factorisations of $O(N^{\theta+\epsilon})$ numbers close to N with the factorisations of the first $O(N^{\theta+\epsilon})$ integers. The result given here (with $\theta = 1/3$) is rather crude, because the series (6) and (7) were approximated by trivially computing the partial sum (8). An avenue for improvement would be in the selection of a better suited test function or another (or more than one) multiplicative function.

Acknowledgement: Research supported in part by a grant from the Social Development Fund.

References

[1] P. Borwein. An efficient algorithm for the Riemann zeta function. In *Constructive, experimental, and nonlinear analysis (Limoges, 1999)*, volume 27 of *CRC Math. Model. Ser.*, pages 29–34. CRC, Boca Raton, FL, 2000.
[2] H. Cohen, F. Rodriguez-Villegas, and D. Zagier. Convergence acceleration of alternating series. *Exp. Math.*, 9(1):3–12, 2000.
[3] H. Davenport. *Multiplicative Number Theory*, volume 74 of *Graduate Texts in Mathematics*. Springer Verlag, 1980.
[4] M. Hittmeir. A babystep-giantstep method for faster deterministic integer factorization. *Math. Comput.*, 87(314):2915–2935, 2018.
[5] A. K. Lenstra, H. W. Lenstra Jr., M. S. Manasse, and J. M. Pollard. The Number Field Sieve. In *ACM Symposium on Theory of Computing*, pages 564–572, 1990.
[6] A. K. Lenstra and H. W. Lenstra, Jr., editors. *The development of the number field sieve*, volume 1554 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1993.
[7] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math. (2)*, 126(3):649–673, 1987.
[8] H. W. Lenstra, Jr. and Carl Pomerance. A rigorous time bound for factoring integers. *J. Amer. Math. Soc.*, 5(3):483–516, 1992.
[9] M. A. Morrison and J. Brillhart. A method of factoring and the factorization of F_7. *Math. Comp.*, 29:183–205, 1975. Collection of articles dedicated to Derrick Henry Lehmer on the occasion of his seventieth birthday.
[10] J. M. Pollard. Theorems on factorization and primality testing. *Proc. Cambridge Philos. Soc.*, 76:521–528, 1974.
[11] C. Pomerance. Analysis and comparison of some integer factoring algorithms. In *Computational methods in number theory, Part I*, volume 154 of *Math. Centre Tracts*, pages 89–139. Math. Centrum, Amsterdam, 1982.