Canad. Math. Bull. Vol. 62 (1), 2019 pp. 81–97
http://dx.doi.org/10.4153/CMB-2018-035-0

Factorization Tests and Algorithms Arising from Counting Modular Forms and Automorphic Representations

Miao Gu and Greg Martin

Abstract. A theorem of Gekeler compares the number of non-isomorphic automorphic representations associated with the space of cusp forms of weight k on $\Gamma_0(N)$ to a simpler function of k and N, showing that the two are equal whenever N is squarefree. We prove the converse of this theorem (with one small exception), thus providing a characterization of squarefree integers. We also establish a similar characterization of prime numbers in terms of the number of Hecke newforms of weight k on $\Gamma_0(N)$.

It follows that a hypothetical fast algorithm for computing the number of such automorphic representations for even a single weight k would yield a fast test for whether N is squarefree. We also show how to obtain bounds on the possible square divisors of a number N that has been found not to be squarefree via this test, and we show how to probabilistically obtain the complete factorization of the squarefull part of N from the number of such automorphic representations for two different weights. If in addition we have the number of such Hecke newforms for even a single weight k, then we show how to probabilistically factor N entirely. All of these computations could be performed quickly in practice, given the number(s) of automorphic representations and modular forms as input.

1 Introduction

An integer is *squarefree* if it is not divisible by the square of any prime. Deciding whether a number is squarefree is trivial if one has its complete factorization; however, we currently lack fast algorithms for factoring large integers, nor do we have any alternate characterization of squarefree numbers that allows for a faster test (unlike the case of polynomials over a field of characteristic 0, for example, where a polynomial is squarefree if and only if it is coprime to its derivative). The origin of this paper is an interesting connection, related to squarefreeness, between the number of certain automorphic representations and the value of a very simple function.

Definition 1.1 Let $A(k,N)$ denote the number of non-isomorphic automorphic representations associated with the space of cusp forms of weight k on $\Gamma_0(N)$. An explicit formula for $A(k,N)$ as a linear combination of multiplicative functions of N, as derived by the second author [5], is given in Proposition 2.5 below. (An equivalent

Received by the editors September 7, 2017; revised June 21, 2018.
Published electronically December 1, 2018.
The second author's work is partially supported by a National Sciences and Engineering Research Council of Canada Discovery Grant.
AMS subject classification: **11F70**, 11N25, 11N60, 11Y05, 11Y16.
Keywords: modular form, automorphic representation, squarefree number, primality testing, factorization algorithm.

way to describe the quantity $A(k,N)$ is the number of weight-k Hecke newforms of level dividing N.)

Definition 1.2 For any positive integer N and any positive even integer k, define

$$G(k,N) = \frac{k-1}{12}N - \frac{1}{2} + c_2(k)\left(\frac{-4}{N}\right) + c_3(k)\left(\frac{-3}{N}\right).$$

The quantities $\left(\frac{-4}{N}\right)$, $\left(\frac{-3}{N}\right)$, $c_2(k)$, and $c_3(k)$ are given in Definitions 2.1 and 2.2; for now, we emphasize that they depend only upon the residue classes of N and k modulo 12. Consequently, $G(k,N)$ can be computed extremely rapidly, even without knowing the factorization of N.

Gekeler [3] proved that the function $G(k,N)$ (for which he gave a different but equivalent expression) is equal to $A(k,N)$ when $N \geq 2$ is squarefree. Our first theorem is a converse of this statement (with one small exception and another small case where the expected inequality is reversed).

Theorem 1.3 *Let $N \geq 2$ be an integer and k a positive even integer.*

- *When N is squarefree, or when $k = 2$ and $N = 9$, we have $G(k,N) = A(k,N)$.*
- *When $k = 2$ and $N = 4$, we have $G(k,N) < A(k,N)$.*
- *In all other cases, we have $G(k,N) > A(k,N)$.*

Corollary 1.4 *Let $N \geq 10$. Then for any positive even integer k, we have that N is squarefree if and only if $A(k,N) = G(k,N)$.*

We pause to dwell upon the hypothetical significance of this corollary. As of the writing of this paper, nobody has found an algorithm that determines whether or not a positive integer N is squarefree that is significantly faster than factoring N; in particular, we do not know any polynomial-time algorithm for testing squarefreeness. The standard way to compute $A(k,N)$ is through factoring N (as per the formula in Proposition 2.5). However, if someone were to develop an alternate way to calculate $A(k,N)$ that was much faster, then Corollary 1.4 would provide a fast way to test the number N for squarefreeness. Indeed, it is tantalizing to observe that such an alternate calculation of $A(k,N)$ need not be particularly robust: *a polynomial-time algorithm for calculating, given a number N, even one single value of $A(k,N)$—perhaps for a special even number k depending upon N—would yield a polynomial-time algorithm for testing whether N is squarefree* (as long as k were not astronomically large). We could even obtain the same outcome with a fast algorithm yielding a sufficiently good upper bound for $A(k,N)$, or one that calculated a positive linear combination of $A(k,N)$ for several values of k. It is admittedly difficult to speculate about what such an algorithm would entail: any method that actually enumerated Hecke eigenforms, for example, would be slower than factoring N in practice, because the number of such eigenforms is essentially linear in N (and hence exponentially large in the length of N).

One can extract more information from this idea than simply whether N is squarefree. For example, in Proposition 3.4, we give upper and lower bounds (depending upon the difference between $G(k,N)$ and $A(k,N)$ for a single value of k) for the size of any integer d whose square divides N. If we have access to two distinct values of

https://doi.org/10.4153/CMB-2018-035-0 Published online by Cambridge University Press

$A(k,N)$ for the same number N, we can do even better, as the next theorem demonstrates. Recall that an integer is *squarefull* if every prime dividing it divides it to at least the second power; every number N has a unique factorization of the form $N = EL$ where E is squarefree, L is squarefull, and $\gcd(E,L) = 1$.

Theorem 1.5 *Let N be a positive integer. Suppose we know two values $A(k_1,N)$ and $A(k_2,N)$ for distinct positive even integers k_1 and k_2. Then we can quickly obtain the complete factorization of the squarefull part of N. More precisely, we can, in probabilistic polynomial time, calculate distinct primes $p_1,\dots,p_\ell$, integers $e_1,\dots,e_\ell \geq 2$, and a squarefree number E that is relatively prime to $p_1\cdots p_\ell$, satisfying $N = Ep_1^{e_1}\cdots p_\ell^{e_\ell}$.*

(The theorem is valid, though uninteresting, when N itself is squarefree, since $\ell = 0$ is permitted. We remark that it would suffice to have two values $A(k_1,M)$ and $A(k_2,M)$ for any multiple M of N, since one can easily deduce the factorization of the squarefull part of N from the factorization of the squarefull part of M.) We do not explicitly report the complexity of the polynomial-time algorithms in this paper, although many of them are extremely fast in practice.

As far as we are aware, these results represent the first known applications of enumerative results in the theory of automorphic representations to computational complexity questions related to integer factorization. In this vein, it seems worth pointing out a similar application of the dimension of the space of cusp forms on $\Gamma_0(N)$ to primality testing (even though, in contrast to deciding whether a number is squarefree, primality testing is already in quite an acceptable state).

Definition 1.6 Let $B(k,N)$ denote the dimension of the space of weight-k newforms on $\Gamma_0(N)$. (The function $B(k,N)$ is often denoted by $g_0^{\#}(k,N)$; an explicit formula for this function as a linear combination of multiplicative functions of N was given by the second author [5, Theorem 1] and is summarized in Proposition 5.1.)

Definition 1.7 Define the function

$$H(k,N) = G(k,N) - B(k,1) = G(k,N) - \left(\frac{k-7}{12} + c_2(k) + c_3(k) + \delta_2(k)\right),$$

where $G(k,N)$ is as in Definition 1.2; note that $H(k,N)$ can be computed extremely rapidly, even without knowing the factorization of N.

Our second theorem demonstrates that a polynomial-time algorithm for calculating $B(k,N)$ would yield a very fast algorithm for testing whether N is prime.

Theorem 1.8 *Let $N \geq 2$ be an integer and let k be a positive even integer.*

- *When N is prime, or when $k = 4$ and $N = 6$, or when $k = 2$ and $N = 6$, 9, 10, 14, 15, 21, 26, 35, 39, 65, or 91, we have $H(k,N) = B(k,N)$.*
- *When $k = 2$ and $N = 4$, we have $H(k,N) < B(k,N)$.*
- *In all other cases, we have $H(k,N) > B(k,N)$.*

Corollary 1.9 *Let $N \geq 92$. Then for any positive even integer k, we have that N is prime if and only if $H(k,N) = B(k,N)$.*

https://doi.org/10.4153/CMB-2018-035-0 Published online by Cambridge University Press

Of course, a deterministic polynomial-time primality test already exists [1], and we have very fast probabilistic primality tests (although, depending upon the speed of the hypothetical oracle that calculates $B(k,N)$, the test resulting from Corollary 1.9 could be even faster). However, if we combine the ideas from the proofs of the previous theorems, we can actually produce a fast method for factoring integers.

Theorem 1.10 *Let N be a positive integer. Suppose we know two values, $A(k_1,N)$ and $A(k_2,N)$, for distinct positive even integers k_1 and k_2, and a value $B(k,N)$ for some positive even integer k. Then we can calculate the complete factorization of N in probabilistic polynomial time.*

As remarked after Theorem 1.5, it would suffice to know values $A(k_1,M)$, $A(k_2,M)$, and $B(k,M)$ for any multiple M of N.

We establish Theorem 1.3 in the next section. In Section 3 we establish upper and lower bounds for square divisors of N based on the difference between $G(k,N)$ and $A(k,N)$. Thereafter, we prove Theorem 1.5 in Section 4, Theorem 1.8 in Section 5, and Theorem 1.10 in Section 6.

2 Testing for Squarefreeness

In this section we establish Theorem 1.3. We begin by giving an explicit formula (Proposition 2.5) for $A(k,N)$; to do so, we must start with several definitions of functions appearing in that formula, as well as in Definition 1.2 for $G(k,N)$. After establishing sufficient notation and recording a useful lower bound for $G(k,N)-A(k,N)$, we establish Theorem 1.3 via Lemmas 2.8–2.10.

Definition 2.1 $\left(\frac{-4}{N}\right)$ and $\left(\frac{-3}{N}\right)$ are special values of the Kronecker symbol:

$$\left(\frac{-4}{N}\right)=\begin{cases}1 & \text{if } N\equiv 1 \pmod 4,\\ -1 & \text{if } N\equiv 3 \pmod 4,\\ 0 & \text{if } 2\mid N;\end{cases}\qquad \left(\frac{-3}{N}\right)=\begin{cases}1 & \text{if } N\equiv 1 \pmod 3,\\ -1 & \text{if } N\equiv 2 \pmod 3,\\ 0 & \text{if } 3\mid N.\end{cases}$$

Definition 2.2 The functions c_2 and c_3 are defined as follows:

$$c_2(k)=\frac{1}{4}+\left\lfloor\frac{k}{4}\right\rfloor-\frac{k}{4}=\begin{cases}1/4 & \text{if } k\equiv 0 \pmod 4,\\ -1/4 & \text{if } k\equiv 2 \pmod 4;\end{cases}$$

$$c_3(k)=\frac{1}{3}+\left\lfloor\frac{k}{3}\right\rfloor-\frac{k}{3}=\begin{cases}1/3 & \text{if } k\equiv 0 \pmod 3,\\ 0 & \text{if } k\equiv 1 \pmod 3,\\ -1/3 & \text{if } k\equiv 2 \pmod 3.\end{cases}$$

(We do not list the values of $c_2(k)$ when k is odd, since we consider only even integers k in this paper.) We also define

$$\delta_1(m)=\begin{cases}1 & \text{if } m=1,\\ 0 & \text{if } m\neq 1,\end{cases}\quad\text{and}\quad \delta_2(m)=\begin{cases}1 & \text{if } m=2,\\ 0 & \text{if } m\neq 2.\end{cases}$$

https://doi.org/10.4153/CMB-2018-035-0 Published online by Cambridge University Press

Definition 2.3 The multiplicative functions s_0^* and v_∞^* are defined as follows:

$$s_0^*(N) = \prod_{\substack{p^e \| N \\ e \geq 2}} \left(1 - \frac{1}{p^2}\right), \qquad v_\infty^*(N) = \prod_{\substack{p^e \| N \\ e \geq 2}} (p-1)p^{\lfloor e/2 - 1 \rfloor}.$$

In particular, $s_0^*(N) = v_\infty^*(N) = 1$ when N is squarefree. Note that if $M \mid N$, then $s_0^*(M) \geq s_0^*(N)$ and $v_\infty^*(M) \leq v_\infty^*(N)$; in particular, $s_0^*(N) \leq 1 \leq v_\infty^*(N)$ for all positive integers N. We also remark that if D is the largest integer such that $D^2 \mid N$, then $v_\infty^*(N) = \phi(D)$, where ϕ is the Euler phi-function.

Definition 2.4 The multiplicative functions v_2^* and v_3^* are defined in terms of the Kronecker symbol (see Definition 2.1) as follows:

$$v_2^*(N) = \begin{cases} \left(\frac{-4}{N}\right) & \text{if } N \text{ is squarefree,} \\ -\left(\frac{-4}{N/4}\right) & \text{if } 4 \mid N \text{ and } N/4 \text{ is squarefree,} \\ 0 & \text{otherwise;} \end{cases}$$

$$v_3^*(N) = \begin{cases} \left(\frac{-3}{N}\right) & \text{if } N \text{ is squarefree,} \\ -\left(\frac{-3}{N/9}\right) & \text{if } 9 \mid N \text{ and } N/9 \text{ is squarefree,} \\ 0 & \text{otherwise.} \end{cases}$$

The following proposition was derived by the second author [5, Theorem 4]. (In that paper, the function $A(k, N)$ was denoted by $g_0^*(k, N)$, but that notation would be confusing in the present context. It can be quickly verified that the formulas given in Definitions 2.3 and 2.4 are equivalent to those given in [5, Definition 4′].)

Proposition 2.5 *For any integer $N \geq 2$ and any even integer $k \geq 2$,*

$$A(k, N) = \frac{k-1}{12} N s_0^*(N) - \frac{1}{2} v_\infty^*(N) + c_2(k) v_2^*(N) + c_3(k) v_3^*(N).$$

We now characterize the values of k and N for which the actual number $A(k, N)$ of non-isomorphic automorphic representations equals the simpler function $G(k, N)$ from Gekeler's theorem.

Definition 2.6 Define $\Delta(k, N) = G(k, N) - A(k, N)$. From Definition 1.2 and Proposition 2.5, we see that for any integer $N \geq 2$ and any even integer $k \geq 2$,

$$\Delta(k, N) = \frac{k-1}{12} N\left(1 - s_0^*(N)\right) + \frac{1}{2}\left(v_\infty^*(N) - 1\right) + c_2(k)\left(\left(\frac{-4}{N}\right) - v_2^*(N)\right) + c_3(k)\left(\left(\frac{-3}{N}\right) - v_3^*(N)\right). \tag{2.1}$$

Our intuition should be that square divisors of N cause the first two terms on the right-hand side of equation (2.1) to be significantly positive. We proceed to make this strategy precise.

https://doi.org/10.4153/CMB-2018-035-0 Published online by Cambridge University Press

Lemma 2.7 *For any integer $N \geq 2$ and any even integer $k \geq 2$,*

$$\Delta(k,N) \geq \frac{k-1}{12} N\big(1 - s_0^*(N)\big) + \frac{1}{2} v_\infty^*(N) - \frac{13}{12}. \tag{2.2}$$

Proof We easily verify that

$$\left(\frac{-4}{N}\right) - v_2^*(N) = \begin{cases} 0 & \text{if } N \text{ is squarefree,} \\ \left(\frac{-4}{N/4}\right) & \text{if } 4 \mid N \text{ and } N/4 \text{ is squarefree,} \\ \left(\frac{-4}{N}\right) & \text{otherwise;} \end{cases}$$

$$\left(\frac{-3}{N}\right) - v_3^*(N) = \begin{cases} 0 & \text{if } N \text{ is squarefree,} \\ \left(\frac{-3}{N/9}\right) & \text{if } 9 \mid N \text{ and } N/9 \text{ is squarefree,} \\ \left(\frac{-3}{N}\right) & \text{otherwise.} \end{cases}$$

In particular,

$$\left| c_2(k)\left(\left(\frac{-4}{N}\right) - v_2^*(N)\right)\right| \leq \frac{1}{4} \quad \text{and} \quad \left| c_3(k)\left(\left(\frac{-3}{N}\right) - v_3^*(N)\right)\right| \leq \frac{1}{3}.$$

The inequality (2.2) now follows immediately from the formula (2.1). ∎

In the current notation, Theorem 1.3 characterizes the sign of $\Delta(k,N)$ in terms of k and N. Gekeler's theorem already tells us that $\Delta(k,N) = 0$ when $N \geq 2$ is squarefree; this fact can be quickly verified by noting that all four summands on the right-hand side of equation (2.1) vanish when N is squarefree, thus reproving Gekeler's theorem as a corollary of Proposition 2.5.

At this point, then, to establish Theorem 1.3, it remains only to prove that if N is not squarefree, then $\Delta(k,N) > 0$, except for the two exceptions $\Delta(2,9) = 0$ and $\Delta(2,4) = -\frac{1}{2}$. We accomplish this via the next three lemmas, distinguished by the size of the prime whose square divides N.

Lemma 2.8 *Let N be a positive integer and let $k \geq 2$ be an even integer. If there exists a prime $p \geq 5$ such that $p^2 \mid N$, then $\Delta(k,N) > 0$.*

Proof Since $s_0^*(N) \leq 1$ for all positive integers N, we can simplify inequality (2.2) to

$$\Delta(k,N) \geq \frac{1}{2} v_\infty^*(N) - \frac{13}{12}.$$

But the fact that $p^2 \mid N$ implies that $v_\infty^*(p^2) \leq v_\infty^*(N)$, and therefore

$$\Delta(k,N) \geq \frac{1}{2} v_\infty^*(p^2) - \frac{13}{12} = \frac{p-1}{2} - \frac{13}{12},$$

which is positive thanks to the assumption $p \geq 5$. ∎

Lemma 2.9 *Let N be a positive integer and let $k \geq 2$ be an even integer. If $9 \mid N$, then $\Delta(k,N) > 0$ unless $k = 2$ and $N = 9$.*

https://doi.org/10.4153/CMB-2018-035-0 Published online by Cambridge University Press

Proof The fact that $9 \mid N$ implies that $s_0^*(9) \geq s_0^*(N)$ and $v_\infty^*(9) \leq v_\infty^*(N)$, and hence Lemma 2.7 implies

$$\Delta(k,N) \geq \frac{k-1}{12}N\big(1-s_0^*(9)\big) + \frac{1}{2}v_\infty^*(9) - \frac{13}{12} = \frac{(k-1)N}{108} - \frac{1}{12}.$$

The right-hand side is automatically positive when $(k-1)N > 9$; given the assumption $9 \mid N$, the only case left to check (since k is a positive even integer) is $\Delta(2,9) = 0$. ∎

Lemma 2.10 *Let N be a positive integer and let $k \geq 2$ be an even integer. If $4 \mid N$, then $\Delta(k,N) > 0$ unless $k = 2$ and $N = 4$.*

Proof The fact that $4 \mid N$ implies that $s_0^*(4) \geq s_0^*(N)$ and $v_\infty^*(4) \leq v_\infty^*(N)$, and hence Lemma 2.7 implies

$$\Delta(k,N) \geq \frac{k-1}{12}N\big(1-s_0^*(4)\big) + \frac{1}{2}v_\infty^*(4) - \frac{13}{12} = \frac{(k-1)N}{48} - \frac{7}{12}.$$

The right-hand side is automatically positive when $(k-1)N > 28$; given the assumption $4 \mid N$, the only cases left to check (since k is a positive even integer) are $\Delta(2,4) = -\frac{1}{2}$ and $\Delta(2,8) = \Delta(2,12) = \Delta(2,16) = \Delta(2,20) = \Delta(2,24) = \Delta(2,28) = \Delta(4,4) = \Delta(4,8) = \Delta(6,4) = \Delta(8,4) = \frac{1}{2}$. ∎

The proof of Theorem 1.3 is now complete.

3 Bounds for the Size of Square Divisors

Theorem 1.3 tells us that a single value $A(k,N)$ is enough to determine whether or not the number N is squarefree. In this section, we show that even more detailed information can be obtained from $A(k,N)$: we can place upper and lower bounds upon the possible square factors of N. We provide explicit upper and lower bounds for such divisors in Proposition 3.4, and asymptotic versions of those bounds in Proposition 3.5. The latter statement, in particular, makes it clear that these bounds are best when $A(k,N)$ is close to $G(k,N)$; in the course of the proof we will see that their difference cannot be significantly smaller than $\sqrt[3]{N}$ when N is large (equation (3.4) gives a precise inequality of this type). We end this section with an illustration of these bounds for the simplest example of a non-squarefree number N.

Definition 3.1 For the rest of this section, given a positive integer N and a positive even integer k, we will use the notation

$$T_0 = 12\left(\Delta(k,N) + \frac{1}{2} - c_2(k)\left(\frac{-4}{N}\right) - c_3(k)\left(\frac{-3}{N}\right)\right).$$

We see that T_0 is essentially a scaled version of $\Delta(k,N)$: it is easy to check that $|T_0 - 12\Delta(k,N)| \leq 13$, and T_0 can be instantly computed from $\Delta(k,N)$ without requiring the factorization of N. We also define

$$T = \begin{cases} T_0 + 3 & \text{if } 3 \mid k, \\ T_0 + 7 & \text{if } 3 \nmid k. \end{cases}$$

https://doi.org/10.4153/CMB-2018-035-0 Published online by Cambridge University Press

In particular, T can be computed from a given value of $A(k,N)$ in polynomial time (since $G(k,N)$ is trivial to calculate).

Lemma 3.2 *For any positive integer N and any positive even integer k,*

$$T \geq (k-1)N\big(1-s_0^*(N)\big) + 6v_\infty^*(N).$$

Proof Comparing Definition 3.1 and equation (2.1), we see that

$$\begin{aligned} T_0 &= (k-1)N\big(1-s_0^*(N)\big) + 6v_\infty^*(N) - 12c_2(k)v_2^*(N) - 12c_3(k)v_3^*(N) \\ &\geq (k-1)N\big(1-s_0^*(N)\big) + 6v_\infty^*(N) - \begin{cases} 3 & \text{if } 3 \mid k, \\ 7 & \text{if } 3 \nmid k, \end{cases} \end{aligned}$$

by Definitions 2.2 and 2.4. This inequality is equivalent to the statement of the lemma. ∎

Definition 3.3 Given a positive integer N and a positive even integer k, we will also use the notation

$$\mathcal{L} = e^\gamma \log\log\sqrt{N} + \frac{2.50637}{\log\log\sqrt{N}},$$

$$\theta = \arccos\Big(1 - \frac{486(k-1)N}{\mathcal{L}^2 T^3}\Big),$$

where $\gamma \approx 0.577$ is Euler's constant; note that $\mathcal{L}$ is positive when $N \geq 10$. (We will see that in our application, θ is always well defined.)

We emphasize that T, $\mathcal{L}$, and θ all depend on k and N, though we have suppressed that dependence from the notation for the sake of readability.

The following proposition gives explicit, easily computable, upper and lower bounds (given a value $A(k,N)$) for integers whose square divides N.

Proposition 3.4 *Let N be a positive integer. If $d \geq 27$ is an integer such that $d^2 \mid N$, then*

$$\frac{\mathcal{L}T}{9}\cos\Big(\frac{\theta}{3} - \frac{2\pi}{3}\Big) + \frac{\mathcal{L}T}{18} < d < \frac{\mathcal{L}T}{9}\cos\frac{\theta}{3} + \frac{\mathcal{L}T}{18},$$

where $\mathcal{L}$, T, and θ are as in Definitions 3.1 and 3.3.

Proof Since $d^2 \mid N$, by Definition 2.3 we have

$$\frac{d^2-1}{d^2} \geq \frac{1}{d^2}\prod_{p^e \parallel d}(p^{2e}-1) = \prod_{p^e \parallel d}\frac{p^{2e}-1}{p^{2e}} \geq \prod_{p \mid d}\frac{p^2-1}{p^2} = s_0^*(d^2) \geq s_0^*(N),$$

and consequently $1 - s_0^*(N) \geq 1/d^2$. Furthermore, if we let D be the largest integer such that $D^2 \mid N$, then again by Definition 2.3,

$$v_\infty^*(N) = \phi(D) \geq \phi(d) > \frac{d}{e^\gamma \log\log d + 2.50637/\log\log d} \geq \frac{d}{\mathcal{L}},$$

where $\mathcal{L}$ is as in Definition 3.3. Here the middle inequality is an explicit upper bound for $d/\phi(d)$ by Rosser–Schoenfeld [6, Theorem 15], and the last inequality is due to the

https://doi.org/10.4153/CMB-2018-035-0 Published online by Cambridge University Press

fact that $d \le \sqrt{N}$ and that the function $e^{\gamma}\log\log x + 2.50637/\log\log x$ is increasing for $x \ge 27$. Therefore by Lemma 3.2,

$$T \ge (k-1)N\big(1 - s_0^*(N)\big) + 6v_\infty^*(N) > \frac{(k-1)N}{d^2} + \frac{6d}{\mathcal{L}} \tag{3.1}$$

or equivalently

$$-\frac{6}{\mathcal{L}}d^3 + Td^2 - (k-1)N > 0. \tag{3.2}$$

Consider the cubic polynomial $f(x) = -\frac{6}{\mathcal{L}}x^3 + Tx^2 - (k-1)N$. The value $f(0)$ is negative, while $f(x)$ is positive when x is sufficiently negative; therefore, $f(x)$ has a negative root. On the other hand, $f(d)$ is positive by equation (3.2), while $f(x)$ is negative when x is sufficiently positive. Therefore $f(x)$ has three real roots x_0, x_1, x_2. The trigonometric form of Cardano's formula (see [2, equation A1.23]) yields an exact expression for these three roots:

$$x_j = \frac{\mathcal{L}T}{9}\cos\Big(\frac{\theta}{3} - \frac{2j\pi}{3}\Big) + \frac{\mathcal{L}T}{18}, \quad j = 0, 1, 2,$$

where θ is as in Definition 3.3. One can check that $x_2 \le 0 \le x_1 \le x_0$. Since d is positive, the inequality (3.2) forces $x_1 < d < x_0$, which is the statement of the lemma. ∎

The results of the previous proposition can be converted into asymptotic bounds whose sizes are easier to gauge (although less suited for explicit computation).

Proposition 3.5 *Let N be a positive integer. If $d \ge 27$ is an integer such that $d^2 \mid N$, then*

$$\sqrt{\frac{(k-1)N}{12\Delta(k,N)}} + O\Big(\frac{kN}{\Delta(k,N)^2\log\log N}\Big) \le d$$
$$< 2e^{\gamma}\Delta(k,N)\log\log N + O\Big(\frac{\Delta(k,N)}{\log\log N} + \log\log N\Big).$$

Proof We first claim that

$$\sqrt{\frac{(k-1)N}{T}} + O\Big(\frac{kN}{\mathcal{L}T^2}\Big) \le d < \frac{\mathcal{L}T}{6}. \tag{3.3}$$

The upper bound follows directly from $T > 6d/\mathcal{L}$, which is a consequence of equation (3.1), or from the right-hand inequality in Proposition 3.4. As for the lower bound, we use the Puiseux series approximation

$$\cos\Big(\frac{\arccos(1-x)}{3} - \frac{2\pi}{3}\Big) = -\frac{1}{2} + \sqrt{\frac{x}{6}} + O(x),$$

https://doi.org/10.4153/CMB-2018-035-0 Published online by Cambridge University Press

with $x = 486(k-1)N/\mathcal{L}^2T^3$ (so that $\theta = \arccos(1-x)$ by Definition 3.3), in the left-hand inequality of Proposition 3.4. We obtain

$$d \geq \frac{\mathcal{L}T}{9}\Big(-\frac{1}{2} + \sqrt{\frac{486(k-1)N/\mathcal{L}^2T^3}{6} + O\Big(\frac{486(k-1)N}{\mathcal{L}^2T^3}\Big)}\Big) + \frac{\mathcal{L}T}{18}$$
$$= \sqrt{\frac{(k-1)N}{T}} + O\Big(\frac{kN}{\mathcal{L}T^2}\Big)$$

as claimed.

Note that equation (3.1) implies

$$T > \frac{(k-1)N}{d^2} + \frac{6d}{\mathcal{L}} \geq \sqrt[3]{\frac{243(k-1)N}{\mathcal{L}^2}} \tag{3.4}$$

by calculus or a weighted arithmetic mean/geometric mean inequality. The hypotheses of the proposition force $N \geq 27^2$, and the right-hand side of equation (3.4) is an increasing function of N in this range; from these inequalities (and $k \geq 2$) we deduce that $T > 21$. In particular, since $|T - 12\Delta(k,N)| \leq 20$, we are justified in writing $T = 12\Delta(k,N)(1 + O(1/\Delta(k,N)))$. From Definition (3.3), we can also write $\mathcal{L} = (1+O(1/(\log\log N)^2))e^{\gamma}\log\log N$. These last two approximations convert equation (3.3) into the asymptotic form asserted by the proposition. ∎

We illustrate this last proposition with an example. Suppose that $N = Ep^2$, where $p > 3$ is prime and $E \equiv 1 \pmod{12}$ is a squarefree number not divisible by p. (For numbers encountered in practice that are not squarefree but have no square factors that are easily found through direct computation, this factorization type is by the far the most likely. The simplifying assumption $E \equiv 1 \pmod{12}$ is solely for the purposes of exposition.) The various multiplicative functions in the definitions of $G(k,N)$ and $A(k,N)$ take the following values: $s_0^*(N) = 1 - \frac{1}{p^2}$ and $v_\infty^*(N) = p-1$, while $\left(\frac{-4}{N}\right) = \left(\frac{-3}{N}\right) = 1$ (since N is also congruent to 1 modulo 12) and $v_2^*(N) = v_3^*(N) = 0$. Consequently, taking $k = 2$,

$$G(2,N) = \frac{1}{12}Ep^2 - \frac{1}{2} - \frac{1}{4} - \frac{1}{3} \quad \text{and} \quad A(2,N) = \frac{1}{12}E(p^2-1) - \frac{1}{2}(p-1),$$

and therefore

$$\Delta(2,N) = \frac{E + 6p - 19}{12}.$$

From this evaluation, we see that if $p \asymp N^{\alpha}$, then $\Delta(2,N) \asymp N^{1-2\alpha}$ when $\alpha \leq \frac{1}{3}$, while $\Delta(2,N) \asymp N^{\alpha}$ when $\alpha \geq \frac{1}{3}$.

When $\alpha \leq \frac{1}{3}$, so that $\Delta(2,N) \asymp N^{1-2\alpha}$, the lower bound on $d = p$ in Proposition 3.5 is $\asymp N^{\alpha}$, while the upper bound is $\asymp N^{1-2\alpha}\log\log N$; in particular, p is quite close to the lower bound. On the other hand, when $\alpha > \frac{1}{3}$, so that $\Delta(2,N) \asymp N^{\alpha}$, the lower bound in Proposition 3.5 is $\asymp N^{(1-\alpha)/2}$ while the upper bound is $\asymp N^{\alpha}\log\log N$; in particular, p is quite close to the upper bound. In either case, one of the two bounds is always rather sharp in this example. (The bounds, while remaining valid, can become less sharp if the squarefull part of N is more complicated.)

https://doi.org/10.4153/CMB-2018-035-0 Published online by Cambridge University Press

4 Factorization of the Squarefull Part

Until now, we have investigated the consequences of having one calculated value of $A(k,N)$. Theorem 1.5 goes further, asserting that we can completely factor the squarefull part of a number N with access to two calculated values of $A(k,N)$. After three preliminary lemmas, we prove Theorem 1.5 at the end of this section.

Lemma 4.1 *Let $N > 1$ be an integer. Given the values $s_0^*(N)$ and $v_\infty^*(N)$ (as in Definition 2.3), the complete factorization of the squarefull part of N can be found in probabilistic polynomial time.*

Proof Write $N = EL$ as the product of its squarefree part E and its squarefull part L with $(E,L) = 1$, and note that we know the quantities $s_0^*(L) = s_0^*(N)$ and $v_\infty^*(L) = v_\infty^*(N)$. We claim that it suffices to find a divisor $d > 1$ of L that we can factor completely. For if we have such a divisor d, then from its prime factors we can easily compute a factorization $N = bn$, where $(b,n) = 1$ and the primes dividing b are exactly the primes dividing d. (Sometimes one writes $b = \gcd(d^\infty, N)$ to describe this factor.) We can then compute $s_0^*(n) = s_0^*(N)/s_0^*(b)$ and $v_\infty^*(n) = v_\infty^*(N)/v_\infty^*(b)$ from the known values $s_0^*(N)$ and $v_\infty^*(N)$ and directly from the definitions of $s_0^*(b)$ and $v_\infty^*(b)$, and then repeat recursively (setting $N = n$) until $n = 1$. There are $o(\log N)$ prime factors of N initially, which means that the number of divisions/multiplications needed in each calculation in this procedure, as well as the number of recursive calls to the procedure itself, are $\ll \log N$; and the integers that appear, along with the numerators and denominators of the rational numbers that appear, are all bounded by N. (This utilization of the divisor d is completely deterministic.)

To find such a divisor d, we simply set d equal to the denominator of $s_0^*(L)$. This denominator cannot equal 1, since $0 < s_0^*(L) < 1$ (here we use the fact that L is squarefull, so that even during the recursion we always have $s_0^*(L) < 1$), and by Definition 2.3 it is clearly a divisor of $\prod_{p|L} p^2$ which itself divides L. On the other hand, note that $dv_\infty^*(L) = d\prod_{p^e \| L}(p-1)p^{\lfloor e/2-1 \rfloor}$ is a multiple of $d\prod_{p|d}(p-1)$, which in turn is a multiple of $\phi(d)$. All that remains is to use the fact, well known to cryptographers (see [7, Section 10.4]), that given a number d and a multiple of $\phi(d)$, there is a probabilistic polynomial-time algorithm for factoring d. ∎

Our general strategy, therefore, is to use two known values of $A(k,N)$ to determine the values $s_0^*(N)$ and $v_\infty^*(N)$, so that the above lemma can be applied. However, the definition of $A(k,N)$ also includes the two other multiplicative functions $v_2^*(N)$ and $v_3^*(N)$. In the next two lemmas we show that we can determine the values of these simpler functions directly from $A(k,N)$.

Lemma 4.2 *Let k be a positive even integer, and let N be a positive integer.*

(i) *Suppose that $9 \mid N$ but $27 \nmid N$. Then $N/9$ is squarefree if and only if*

$$A(k,N) = \frac{2(k-1)}{27}N - 1 - c_3(K)\left(\frac{-3}{N/9}\right). \tag{4.1}$$

https://doi.org/10.4153/CMB-2018-035-0 Published online by Cambridge University Press

(ii) *Suppose that* $4 \mid N$ *but* $8 \nmid N$. *Then* $N/4$ *is squarefree if and only if*

$$A(k,N) = \frac{k-1}{16}N - \frac{1}{2} - c_2(K)\left(\frac{-4}{N/4}\right). \tag{4.2}$$

Proof By direct calculation, we can assume that $N \geq 38$. Proposition 2.5 immediately implies both the equality (4.1) when $\frac{N}{9}$ is squarefree and the equality (4.2) when $\frac{N}{4}$ is squarefree, so it remains only to prove the converses. In part (i), equality (4.1) can be written as

$$\frac{k-1}{12}Ns_0^*(N) - \frac{1}{2}v_\infty^*(N) + c_3(k)v_3^*(N) = \frac{2(k-1)}{27}N - 1 - c_3(k)\left(\frac{-3}{N/9}\right)$$

(we know that $v_2^*(N) = 0$, since $9 \mid N$), or equivalently

$$\frac{k-1}{12}N\left(\frac{8}{9} - s_0^*(N)\right) + \frac{v_\infty^*(N)+2}{2} = c_3(k)\left(v_3^*(N) + \left(\frac{-3}{N/9}\right)\right) + 2.$$

Suppose, for the sake of contradiction, that $\frac{N}{9}$ is not squarefree. Choose a prime p such that $p^2 \mid \frac{N}{9}$, and note that $p \neq 3$, since $27 \nmid N$. Then $s_0^*(N) \leq \frac{8}{9}(1 - \frac{1}{p^2})$ and $v_\infty^*(N) \geq 2(p-1)$ (and $k - 1 \geq 1$), and so

$$\frac{1}{12}N\frac{8}{9p^2} + p \leq c_3(k)\left(v_3^*(N) + \left(\frac{-3}{N/9}\right)\right) + 2 \leq \frac{8}{3}.$$

However, the left-hand side is at least $(\frac{N}{2})^{1/3}$ (for any positive real number p, by an easy calculus exercise). Therefore, we must have $N \leq 2(\frac{8}{3})^3 < 38$, a contradiction. The proof of part (ii) is similar, starting from the given equality

$$\frac{k-1}{12}Ns_0^*(N) - \frac{1}{2}v_\infty^*(N) + c_2(k)v_2^*(N) = \frac{k-1}{16}N - \frac{1}{2} - c_2(k)\left(\frac{-4}{N/4}\right)$$

and eventually deducing that

$$\frac{1}{12}N\frac{3}{4p^2} + \frac{p}{2} \leq c_2(k)\left(v_2^*(N) + \left(\frac{-4}{N/4}\right)\right) + 1 \leq \frac{3}{2},$$

forcing $N \leq 32$, which is again a contradiction. ∎

Lemma 4.3 *Let* k *be a positive even integer, and let* N *be a positive integer. Given the value* $A(k,N)$, *we can determine the values* $v_2^*(N)$ *and* $v_3^*(N)$.

Proof When $4 \nmid N$ and $9 \nmid N$, Theorem 1.3 and the known value $A(k,N)$ allow us to decide whether N is squarefree, which is all that is needed to calculate $v_2^*(N)$ and $v_3^*(N)$ in this case. When $9 \mid N$, we immediately know that $v_2^*(N) = 0$, and if $27 \mid N$, then $v_3^*(N) = 0$ as well; if $27 \nmid N$, Lemma 4.2(i) allows us to determine whether $\frac{N}{9}$ is squarefree, which is what is needed to calculate $v_3^*(N)$. Finally, when $4 \mid N$, we immediately know that $v_3^*(N) = 0$, and if $8 \mid N$, then $v_2^*(N) = 0$ as well; if $8 \nmid N$, Lemma 4.2(ii) allows us to determine whether $\frac{N}{4}$ is squarefree, which is what is needed to calculate $v_2^*(N)$. ∎

https://doi.org/10.4153/CMB-2018-035-0 Published online by Cambridge University Press

Proof of Theorem 1.5 Define $A^*(k,N) = A(k,N) - c_2(k)v_2^*(N) - c_3(k)v_3^*(N)$, and note that $A^*(k,N)$ can be calculated easily from $A(k,N)$ by Lemma 4.3. In this notation, Proposition 2.5 implies that

$$A^*(k_1,N) = \frac{k_1-1}{12}Ns_0^*(N) - \frac{1}{2}v_\infty^*(N),$$
$$A^*(k_2,N) = \frac{k_2-1}{12}Ns_0^*(N) - \frac{1}{2}v_\infty^*(N).$$

This system of two linear equations in the two unknown quantities $s_0^*(N)$ and $v_\infty^*(N)$ can be easily solved in (deterministic) polynomial time, giving quantities that are trivial to calculate from the hypothesized known values:

$$s_0^*(N) = \frac{12\big(A^*(k_2,N) - A^*(k_1,N)\big)}{(k_2-k_1)N},$$
$$v_\infty^*(N) = \frac{2\big(A^*(k_2,N)(k_1-1) - A^*(k_1,N)(k_2-1)\big)}{k_2-k_1}.$$

Therefore, by Lemma 4.1, we can obtain the factorization of the squarefull part of N in probabilistic polynomial time, as claimed. ∎

5 Testing for Primality

In this section we establish Theorem 1.8 concerning the function $B(k,N)$ given in Definition 1.6. Similarly to $A(k,N)$, an exact formula for $B(k,N)$ as a linear combination of multiplicative functions of N was given by the second author [5]. The following proposition records this formula with just enough precision for our current purposes.

Proposition 5.1 *For any positive integer N and any positive even integer k,*

$$B(k,N) = \frac{k-1}{12}Ns_0^\#(N) - \frac{1}{2}v_\infty^\#(N) + c_2(k)v_2^\#(N) + c_3(k)v_3^\#(N) + \delta_2(k)\mu(N), \tag{5.1}$$

where μ is the Möbius mu-function; c_2, c_3, and δ_2 are as in Definition 2.2; and $s_0^\#$, $v_\infty^\#$, $v_2^\#$, and $v_3^\#$ are certain multiplicative functions satisfying the following:

(i) $Ns_0^\#(N) = \phi(N)$ *when N is squarefree;*
(ii) $v_\infty^\#(p) = 0$ *for every prime p;*
(iii) *the only possible values of $v_2^\#(N)$ are 0 and $\pm 2^\ell$ for some integer $0 \le \ell \le \omega(N)$, where $\omega(N)$ is the number of distinct prime factors of N, and similarly for $v_3^\#(N)$;*
(iv) $v_2^\#(p) = \left(\frac{-4}{p}\right) - 1$ *and* $v_3^\#(p) = \left(\frac{-3}{p}\right) - 1$ *for every prime p, where these Kronecker symbols are as in Definition 2.1.*

Proof The given formula appears as [5, Theorem 1] (in which $B(k,N)$ is denoted by $g_0^\#(k,N)$). The exact definitions of the multiplicative functions $s_0^\#$, $v_2^\#$, $v_3^\#$, and $v_\infty^\#(N)$ are given in [5, Definition 1′], from which the listed properties follow immediately. ∎

https://doi.org/10.4153/CMB-2018-035-0 Published online by Cambridge University Press

Corollary 5.2 *Let k be a positive even integer. When N is squarefree,*

$$B(k,N) = \frac{(k-1)\phi(N)}{12} - \frac{\delta_1(N)}{2} + c_2(k)v_2^{\#}(N) + c_3(k)v_3^{\#}(N) + \delta_2(k)\mu(N),$$

where δ_1 is as in Definition 2.2. In particular,

$$B(k,1) = \frac{k-7}{12} + c_2(k) + c_3(k) + \delta_2(k),$$

$$B(k,p) = \frac{(k-1)(p-1)}{12} + c_2(k)v_2^{\#}(p) + c_3(k)v_3^{\#}(p) - \delta_2(k), \tag{5.2}$$

$$B(k,pq) = \frac{(k-1)(p-1)(q-1)}{12} + c_2(k)v_2^{\#}(p)v_2^{\#}(q) + c_3(k)v_3^{\#}(p)v_3^{\#}(q) + \delta_2(k), \tag{5.3}$$

for any distinct primes p and q.

Proof These identities are direct consequences of Proposition 5.1, using the assumption that N is squarefree and the fact that $v_\infty^{\#}$, $v_2^{\#}$, and $v_3^{\#}$ are multiplicative functions. ∎

Corollary 5.3 *Let k be a positive even integer. For any prime p, we have $B(k,p) > 0$, except for the pairs*

$$(k,p) = (2,2), (2,3), (2,5), (2,7), (2,13), (4,2), (4,3), (6,2), \text{ or } (12,2)$$

for which $B(k,p) = 0$. Similarly, for any distinct primes p and q, we have $B(k,pq) > 0$, except that $B(2,6) = B(2,10) = B(2,22) = 0$.

Proof Since $|c_2(k)v_2^{\#}(p) + c_3(k)v_3^{\#}(p) - \delta_2(k)| \le \frac{1}{4}\cdot 2 + \frac{1}{3}\cdot 2 + 1 = \frac{13}{6}$ by Proposition 5.1(iv), the inequality $B(k,p) > 0$ follows from equation (5.2) when $\frac{(k-1)(p-1)}{12} > \frac{13}{6}$, or equivalently when $(k-1)(p-1) > 26$; the finitely many values remaining can be computed individually. Similarly, from equation (5.3) we see that

$$\left| B(k,pq) - \frac{(k-1)(p-1)(q-1)}{12} \right| \le \left(\frac{1}{4}\cdot 4 + \frac{1}{3}\cdot 4 + 1 \right) = \frac{10}{3};$$

therefore, $B(k,pq)$ is positive when $(k-1)(p-1)(q-1) > 40$, and the remaining values can be checked individually. ∎

We remark that these values can also be found on the LMFDB, an online database of information about specific L-functions, modular forms, and related objects [4]

The last fact we need about the function $B(k,N)$ is its relationship to $A(k,N)$. The isomorphism classes of automorphic representations associated with the space of weight-k cusp forms on $\Gamma_0(N)$ are in one-to-one correspondence with weight-k Hecke newforms on $\Gamma_0(d)$ as d ranges over the positive divisors of N. In particular, comparing the cardinalities of these sets results in the well-known convolution formula (see [5, first displayed equation on p. 311])

$$A(k,N) = \sum_{d|N} B(k,d). \tag{5.4}$$

https://doi.org/10.4153/CMB-2018-035-0 Published online by Cambridge University Press

In particular, if N is prime, then by Definition 1.7 and Theorem 1.3 (since primes are squarefree),

$$\begin{aligned} H(k,N) &= G(k,N) - B(k,1) = A(k,N) - B(k,1) \\ &= \big(B(k,N) + B(k,1)\big) - B(k,1) = B(k,N), \end{aligned}$$

which establishes the first assertion of Theorem 1.8. The remaining assertions of Theorem 1.8 are established in the following four lemmas.

Lemma 5.4 *Let $k \geq 2$ be an even integer. If N is a positive integer that is not squarefree, then $H(k,N) > B(k,N)$, except that $H(2,4) < B(2,4)$ and $H(2,9) = B(2,9)$.*

Proof By Definition 1.7 and Theorem 1.3, as long as $(k,N) \neq (2,4)$ and $(k,N) \neq (2,9)$, we have

$$H(k,N) = G(k,N) - B(k,1) > A(k,N) - B(k,1) = \sum_{\substack{d|N \\ d>1}} B(k,d) \geq B(k,N)$$

by equation (5.4), where the last inequality is valid since $N > 1$ and the dimensions $B(k,d)$ are nonnegative. On the other hand, the values $H(2,4) = -\frac{1}{2}$ and $B(2,4) = H(2,9) = B(2,9) = 0$ can be calculated directly. ∎

Lemma 5.5 *Let $N \geq 2$ be a squarefree positive integer and let $k \geq 2$ be an even integer. If there exists a nontrivial divisor d_0 of N (that is, $1 < d_0 < N$ and $d_0 \mid N$) such that $B(k,d_0) > 0$, then $H(k,N) > B(k,N)$.*

Proof By Definition 1.7 and Theorem 1.3,

$$\begin{aligned} H(k,N) &= G(k,N) - B(k,1) = A(k,N) - B(k,1) \\ &= \sum_{\substack{d|N \\ d>1}} B(k,d) \geq B(k,N) + B(k,d_0) > B(k,N) \end{aligned}$$

by equation (5.4), again since the dimensions $B(k,d)$ are nonnegative. ∎

Lemma 5.6 *Let $N \geq 2$ be a squarefree positive integer and let $k \geq 4$ be an even integer. If N is not prime, then $H(k,N) > B(k,N)$, except that $H(4,6) = B(4,6)$.*

Proof Since N is squarefree and not prime, there exist distinct primes $p < q$ dividing N. By Corollary 5.3 we know that $B(k,q)$ is positive, in which case $H(k,N) > B(k,N)$ by Lemma 5.5 with $d_0 = q$. The only exception to this argument is in the case $k = 4$ and $N = 6$, where both $B(4,2)$ and $B(4,3)$ vanish; we verify directly that $H(4,6) = 1 = B(4,6)$. ∎

Lemma 5.7 *Let $N \geq 2$ be a squarefree positive integer. If N is not prime, then $H(2,N) > B(2,N)$ unless $N = 6$, 10, 14, 15, 21, 26, 35, 39, 65, or 91, in which case $H(2,N) = B(2,N)$.*

Proof First suppose that N has at least three distinct prime factors. Then at least two of these primes p, q must be odd; let $d_0 = pq$ be their product, which in particular

https://doi.org/10.4153/CMB-2018-035-0 Published online by Cambridge University Press

is not equal to 6, 10, or 22. By Corollary 5.3, we see that $B(k, d_0) > 0$, and therefore $H(2, N) > B(2, N)$ by Lemma 5.5.

The only remaining case is when $N = pq$ is the product of two distinct primes. If one of these primes is not in the set $\{2, 3, 5, 7, 13\}$, then let d_0 be that prime. By Corollary 5.3, we see that $B(k, d_0) > 0$, and therefore $H(2, N) > B(2, N)$ by Lemma 5.5. Otherwise, both p and q are in the set $\{2, 3, 5, 7, 13\}$, which leads to the $\binom{5}{2} = 10$ values of N listed in the statement of the lemma; and direct computation verifies that $H(2, N) = B(2, N)$ in all ten cases. ∎

The proof of Theorem 1.8 is now complete.

6 Full Factorization

The last result that remains to be established is Theorem 1.10, on factorization the integer N completely using two values of $A(k, N)$ and one value of $B(k, N)$. Fortunately, after the work in the earlier sections, the proof of this theorem is quite brief.

Lemma 6.1 *Let k be a positive even integer. Let E be a positive squarefree integer and let L be a positive squarefull number such that $\gcd(E, L) = 1$, and set $N = EL$. Suppose that we know the value $B(k, N)$, the complete factorization of L, and the values $\nu_2^\#(N)$, $\nu_3^\#(N)$, and $\mu(N)$. Then we can find the complete factorization of E (and hence of N) in probabilistic polynomial time.*

Proof Since the case $E = 1$ is trivial, we may assume that $E > 1$. In this case, there exists at least one prime that divides N to the first power, which gives $\nu_\infty^\#(N) = 0$ by Proposition 5.1(ii). Then by equation (5.1),

$$Ns_0^\#(N) = \frac{12}{k-1}\big(B(k, N) - c_2(k)\nu_2^\#(N) - c_3(k)\nu_3^\#(N) - \delta_2(k)\mu(N)\big),$$

where every term on the right-hand side is known by assumption. We can then compute $Es_0^\#(E) = Ns_0^\#(N)/Ls_0^\#(L)$ from the known value $Ns_0^\#(N)$ and directly from the definition of $Ls_0^\#(L)$. On the other hand, since E is squarefree, Proposition 5.1(i) tells us that $Es_0^\#(E) = \phi(E)$. Therefore, we know the values $E = N/L$ and $\phi(E)$, and hence we can factor E in probabilistic polynomial time (as mentioned in the proof of Lemma 4.1). ∎

Proof of Theorem 1.10 From the two values $A(k_1, N)$ and $A(k_2, N)$, we can obtain (by Theorem 1.5) the factorization of $N = EL$ into its squarefree and squarefull parts, along with the complete factorization of L, in probabilistic polynomial time. Since we also know the value $B(k, N)$, the only obstacle to applying Lemma 6.1 is our ignorance of the values $\nu_2^\#(N)$, $\nu_3^\#(N)$, and $\mu(N)$.

However, by Proposition 5.1(iii), the only possible values for $\nu_2^\#(N)$ and $\nu_3^\#(N)$ are 0 or $\pm 2^\ell$ for some integer $2^\ell \le N$, and of course there are only three possible values for $\mu(N)$. Thus, there are $\ll (\log N)^2$ possible values for the triple $(\nu_2^\#(N), \nu_3^\#(N), \mu(N))$. We simply use each of these possible values (in parallel or in turn) and attempt to apply Lemma 6.1. The computations using incorrect values might result in errors or infinite loops or even incorrect factorizations, but the computation using the correct values will (with high probability) yield the correct

https://doi.org/10.4153/CMB-2018-035-0 Published online by Cambridge University Press

factorization—and any proposed factorization can be quickly checked for correctness. Therefore, these many computations will indeed yield the factorization of N in probabilistic polynomial time. ■

Though we have made no attempt to optimize the running time of the algorithms presented in this paper, it is natural to speculate how one could avoid the need for $O(\log^2 N)$ parallel computations in this last proof. One might expect that, from four values $B(k_j, N)$ for distinct even numbers $k_1, \dots, k_4$, we could use linear algebra to try to solve the system of four equations arising from the formula (5.1) for the four unknown values $Ns_0^\#(N)$, $v_2^\#(N)$, $v_3^\#(N)$, and $\mu(N)$. Indeed, we should even be able to manage with three values $B(k_j, N)$, since the term $\delta_2(k)\mu(N)$ disappears when $L > 1$ (or when $k > 2$), and there are only three possible values for $\delta_2(k)\mu(N)$ in any event.

While this approach works for many triples of weights k_1, k_2, k_3, it does not work in every possible circumstance, because the resulting system of three linear equations in $Ns_0^\#(N)$, $v_2^\#(N)$, and $v_3^\#(N)$ might be degenerate. For example, if

$$(k_1, k_2, k_3) = (12m, 12m + 4, 12m + 8),$$

then any one value among $B(k_1, N), B(k_2, N), B(k_3, N)$ can be calculated from the other two (the middle value is the average of the first and last values, for instance). On the other hand, for certain pairs of weights—for example, if $k_1 \equiv k_2 \pmod{12}$ and $k_1, k_2 > 2$—it is possible to solve for the crucial value $Ns_0^\#(N)$, even though the individual values $v_2^\#(N)$ and $v_3^\#(N)$ are still entangled with each other. In practice, from the explicit formula (5.1), it is an easy matter to determine how much information can be extracted from the values $B(k_j, N)$ for any given weights k_j.

Acknowledgments The authors thank the anonymous referee for several helpful comments and particularly for pointing out the connection to primality tests that led to Theorem 1.8.

References

[1] M. Agrawal, N. Kayal, and N. Saxena, *PRIMES is in P.* Ann. of Math. (2) **160**(2004), no. 2, 781–793. http://dx.doi.org/10.4007/annals.2004.160.781

[2] C. Casandjian, N. Challamel, C. Lanos, and J. Hellesland, *Reinforced concrete beams, columns and frames: mechanics and design*. John Wiley & Sons, Hoboken, NJ, 2013, 267–276. http://dx.doi.org/10.1002/9781118639511

[3] E.-U. Gekeler, *A remark on dimensions of spaces of modular forms.* Arch. Math. (Basel) **65**(1995), no. 6, 530–533. http://dx.doi.org/10.1007/BF01194172

[4] The LMFDB Collaboration, *The L-functions and Modular Forms Database.* http://www.lmfdb.org/ModularForm/GL2/Q/holomorphic

[5] G. Martin, *Dimensions of the spaces of cusp forms and newforms on* $\Gamma_0(N)$ *and* $\Gamma_1(N)$. J. Number Theory **112**(2005), no. 2, 298–331. http://dx.doi.org/10.1016/j.jnt.2004.10.009

[6] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers.* Illinois J. Math. **6**(1962), 64–94.

[7] V. Shoup, *A computational introduction to number theory and algebra*. Cambridge University Press, Cambridge, 2005. http://dx.doi.org/10.1017/CBO9781139165464

Department of Mathematics, Duke University, Durham, NC 27708, USA
Email: miao.gu@duke.edu

Mathematics Department, University of British Columbia, Vancouver, BC V6T 1Z2
Email: gerg@math.ubc.ca