THE HARDNESS OF COMPUTING AN EIGENFORM

ERIC BACH AND DENIS CHARLES

1. Introduction

The Fourier coefficients of modular forms encode very interesting arithmetic data. For example, divisor sums, partition numbers, trace of Frobenius of the reduction modulo primes of an elliptic curve over $\mathbb{Q}$, and more generally, trace of Frobenius of many Galois representations of dimension 2 over finite fields (this being a conjecture of Serre) are all known to be, or conjectured to be, Fourier coefficients of modular forms. A particularly important family of modular forms are the so-called Hecke eigenforms. These are modular forms that are also simultaneous eigenforms for an algebra of operators called the Hecke operators that operate on the spaces of modular forms. The Fourier coefficients of Hecke eigenforms are particularly important arithmetically. Indeed, many of the examples given above arise as Fourier coefficients of Hecke eigenforms.

In this article we are concerned with the computational complexity of computing the Fourier coefficients of these Hecke eigenforms. Currently, there are three approaches to computing the Fourier coefficients of modular forms: a method based on computing theta series of lattices [Piz80]; the method of modular symbols [Mer94, Ste00]; and one based on the Selberg Trace formula (see Cha00 and Chapter 5 of Cha05). All of these methods result in algorithms with exponential running time to compute the Fourier coefficients. The Fourier coefficients of Hecke eigenforms are multiplicative and satisfy recurrences for prime powers. Since there are subexponential time algorithms for factoring integers, the interesting problem is to compute the $p$-th Fourier coefficient, for prime $p$, efficiently. However, this problem is still open in general. For any fixed eigenform of weight 2 one can use Schoof’s algorithm ([Sch85]) for counting points on elliptic curves over finite fields to compute the $p$-th Fourier coefficient efficiently. Recent work of Edixhoven et al. suggests that this approach generalizes to compute eigenforms of weight $k \geq 2$ ([ECdJ+06]).

There have been no hardness results known for computing the Fourier coefficients of eigenforms (except for those of Eisenstein series where the hardness results follow from [BMS86]). In this article, we give evidence that computing Fourier coefficients of the Hecke eigenforms for composite indices is no easier than factoring integers. More precisely, we show that the existence of a polynomial time algorithm that, given $n$, computes the $n$-th Fourier coefficient of a (fixed) Hecke eigenform implies that we can factor most RSA moduli (numbers that are products of two distinct primes) in polynomial time. In particular, our result implies a hardness result for computing the Ramanujan tau function.

1.1. Preliminaries and notation. Since there are a number of excellent references for modular forms we refrain from reproducing the definitions here. Instead, we refer the reader to any of the books [Ser70, Shi71, Lan76, Kob93, Ono04, DS05] for the definition and background on modular forms. The Fourier expansions of modular forms that we refer to are the Fourier expansions at the cusp $\infty$. In the Fourier expansions $q$ stands for $e^{2\pi iz}$. The letters $p$ and $q$ will be used for (rational) prime numbers, the latter will be used when no confusion can arise with the $q$-expansions.

2. The Reduction

Let $S_k(\Gamma_0(N), \chi)$ be the space of cusp forms of even integer weight $k \geq 2$, level $N$, and character $\chi \mod N$. In what follows, fix $f(z) = \sum_{1 \leq n \leq \infty} a(n) q^n \in S_k(\Gamma_0(N), \chi)$ to be a normalized ($a(1) = 1$) Hecke eigenform. We will also assume that $f$ is not of CM type in the sense of Ribet [Rib77]. This means that there does

\begin{footnote}{The condition of even weight is needed for a technical reason in the proof.}

Date: 8 September, 2006.

not exist an imaginary quadratic field, \( L \), such that \( a(p) = 0 \) for all primes \( p \) that are inert in \( L \). Under these assumptions, a beautiful theorem of Serre ([Ser81] Corollary 2 to Theorem 15) gives us bounds on the number of primes \( p \) for which \( a(p) = 0 \).

**Theorem 2.1.** Let \( f(z) = \sum_{n \leq x} a(n)q^n \in S_k(\Gamma_0(N), \chi) \) \((k \geq 2)\) be a normalized Hecke eigenform that is not of CM type. Define \( P_f(x) = \# \{ p \leq x : p \text{ a prime such that } a(p) = 0 \} \). Then

\[
P_f(x) = O \left( \frac{x}{(\log x)^{\frac{k}{2}}} \right) \text{ for all } \delta > 0.
\]

Moreover, if one assumes the Generalized Riemann Hypothesis, we have

\[
P_f(x) = O \left( x^\frac{k}{2} \right).
\]

The assumption that \( f \) not be of CM type is necessary, see Remark 2.6.

The Fourier coefficients of a normalized Hecke eigenform need not be integers, but they are at least algebraic integers (see [Ono04] §2.4 & §2.5; the result also follows from [Shi71] Theorem 3.52). Furthermore, we know that each eigenvalue lies in a number field of degree at most \( \dim S_k(\Gamma_0(N), \chi) \nu(N) \) since the characteristic polynomials of the Hecke operators have degree \( \dim S_k(\Gamma_0(N), \chi) \nu(N) \) over the field \( \mathbb{Q}(\chi) \). In fact, the field \( K_f = \mathbb{Q}(a(2), a(3), \ldots, a(n), \ldots) \) is a number field and so a finite degree extension of \( \mathbb{Q} \). Since \( f \) is fixed we can assume that we can do computations in this field efficiently. We assume that the supposed algorithm that computes the Fourier coefficients takes as input an integer \( n \) and gives us the (monic) minimal polynomial of the \( n \)-th Fourier coefficient \( a(n) \). We also assume that the algorithm provides a complex approximation to \( a(n) \) that distinguishes \( a(n) \) from its conjugates. In other words, we not only have the sub-field \( \mathbb{Q}(a(n)) \subseteq K_f \), but we also have an embedding of \( \mathbb{Q}(a(n)) \) in \( \mathbb{C} \). Since the space \( S_k(\Gamma_0(N), \chi) \) is fixed, and \( \chi \) is a Dirichlet character mod \( N \), we can also compute \( \chi(n) \) for any integer \( n \).

Next, we describe how we can factor RSA moduli if we can compute the Fourier coefficients \( a(n) \). We are given a positive integer \( n = pq \), where \( p, q \) are distinct odd primes. We can also assume (without loss of generality) that \( \gcd(N, n) = 1 \). Let \( x = a(p)/\chi(p)p^{\frac{k-1}{2}} \) and \( y = a(q)/\chi(q)q^{\frac{k-1}{2}} \). Note that we can also assume that \( \chi(n) \neq 0 \) for otherwise \( \gcd(n, N) \neq 1 \). We will make the assumption that \( x \neq 0 \) and \( y \neq 0 \) in the following analysis.

Using the algorithm to compute the Fourier coefficients of \( f \) we can compute

\[
A = a(n) = \frac{xy}{\chi(n)}
\]

and

\[
B = a(n^2).
\]

Now by multiplicativity and the recurrences for prime powers that \( a(n) \) satisfy we have ([Kob93] III.§5)

\[
B = a(n^2) = a(p^2)a(q^2)
\]

(1)

\[
= (a(p)^2 - p^{k-1}\chi(p))(a(q)^2 - q^{k-1}\chi(q))
\]

(2)

\[
= n^{k-1}\chi(n)(x^2 - 1)(y^2 - 1).
\]

(3)

Thus we have a pair of simultaneous equations for \( x \) and \( y \) which we can solve. Setting \( \alpha = A/n^{\frac{k-1}{2}} \) and \( \beta = B/n^{k-1}\chi(n) \), one obtains

\[
x^2 = \frac{\alpha^2 - \beta + 1 \pm \sqrt{(\alpha^2 - \beta + 1)^2 - 4\alpha^2}}{2}
\]

and

\[
y^2 = \frac{\alpha^2}{x^2}.
\]
Substituting the definitions of $\alpha$ and $\beta$ and clearing denominators we get
\[ x^2 = \left( A^2 \chi(n) - B + n^{k-1} \chi(n) \right) \pm \sqrt{\left( A^2 \chi(n) - B + n^{k-1} \chi(n) \right)^2 - 4A^2 n^{k-1} \chi(n)^2}. \]

We note that the radicand is the square of an algebraic integer (see below) and hence the square root can be computed exactly. This can be computed efficiently by computing numerical approximations to the square roots of all the conjugates of radicand. By the definition of $x$ we have that
\[ x^2 = \frac{a(p)^2}{\chi(p)^2 p^{k-1}}. \]

Note that this quantity is not zero under our assumption that $x \neq 0$. We claim that $x^2$ cannot be an algebraic integer if $p$ is large enough. For otherwise, since $k - 1$ is odd, this would make $\sqrt{p}$ an element of $\mathbb{Q}(\chi, a(2), a(3), \ldots, a(n), \ldots)$, but the latter is a finite extension and thus if $p$ is large enough it cannot contain $\sqrt{p}$. Thus we can recover $p$ from the above expression by taking the gcd of the denominator of the above expression with $n$. Since the quantity is an algebraic number the (reduced) denominator in the expression is the leading coefficient of the minimal polynomial over $\mathbb{Z}$.

Suppose $x = 0$ but $y \neq 0$ (i.e. $a(p) = 0$ but $a(q) \neq 0$), we can still proceed as follows. By equation (3) we find that $B = n^{k-1} \chi(n)(1 - y^2)$. Thus we can still get $y^2$ and by the above argument find $q$.

Thus our reduction will succeed in factoring the integer $n$, unless both $a(p)$ and $a(q)$ are zero. Since the set of such primes is density 0 (by Theorem 2.1), we get the following theorem:

**Theorem 2.2.** Let $f(z) = \sum_{1 \leq n \leq k} a(n) q^n \in S_{2k}(\Gamma_0(N), \chi)$ be a normalized Hecke eigenform that is not of CM-type. Suppose there is a polynomial time algorithm that computes $a(n)$ given $n$. Then there is a polynomial time algorithm that factors a density 1 subset of the RSA moduli.

In the case that $f \in S_k(\Gamma_0(N), \chi)$ and $k$ is odd the entire reduction works as long as $p^{k-1}$ does not divide $a(p)$ for one of the primes dividing $n$. The failure of the reduction occurs very rarely. Indeed, if $k \geq 3$ and $k$ is odd then this implies that $a(p) \equiv 0 \mod p$ which means that $p$ is a, so called, non-ordinary prime. A heuristic argument given in [Gou97] shows that the number of non-ordinary primes below $x$ is $O(\log \log x)$. Thus, it is likely that the result of Theorem 2.2 remains true even for odd weight cuspidal eigenforms.

**Example 2.3.** We illustrate the reduction in the case of the Ramanujan Tau function $\tau(n)$ that gives the Fourier coefficients of $\Delta$, a weight 12 eigenform of level 1 and trivial character (see 2.2).

Let $n = 15$, from the tables in [Leh33] one sees that $\tau(15) = 1217160$ and $\tau(15^2) = 2897808426675$. In the notation of the proof of the theorem we have
\[
\alpha^2 = \frac{81288256}{474609375}, \quad \text{and} \quad \beta = \frac{1431016507}{4271484375}.
\]

From this one finds that $x^2 = \frac{3833156}{1953125}$, and $\text{gcd}(1953125, 15) = 5$.

**Example 2.4.** The space $S_4(\Gamma(29))$ with trivial character has a newform, $f$ (say), whose expansion begins $q + \gamma q^2 + (-3\gamma - 8)q^3 + (-2\gamma - 7)q^4 + (4\gamma - 1)q^5 + \cdots$, where $\gamma$ is a root of $x^2 + 2x - 1$. A short computation in MAGMA ([BC03]) tells us that the 15th Fourier coefficient is $-5\gamma - 4$ and that the 225th Fourier coefficient is $-2680\gamma - 6168$. MAGMA computes that either
\[ x^2 = \frac{1}{27}(30\gamma + 73) \text{ or } x^2 = \frac{1}{125}(-40\gamma + 17) \]

corresponding to the two square roots of $(\alpha^2 - \beta + 1)^2 - 4\alpha$ (again we have preserved the notation used in the proof). In any case, the denominators in these expressions yield a proper factor of 15.
Remark 2.5. The hardest cases of factoring the RSA moduli are believed to be those of the form $pq$ where the primes $p$ and $q$ are both approximately the same size. One might wonder if the set of RSA moduli on which our reduction works includes such numbers also. This is indeed true. The number of RSA moduli below a bound $x$ that have both the factors being approximately the same size can be estimated as follows. Let $c$ be a constant with $0 < c < 1$. Using the prime number theorem the number of RSA moduli $pq$ for which $c\sqrt{x} \leq p, q \leq \sqrt{x}$ is

$$\left( \frac{\pi(\sqrt{x}) - \pi(c\sqrt{x})}{2} \right) = \Theta \left( \frac{x}{\log^2 x} \right),$$

where $\pi$ is the prime counting function. Meanwhile, the number of RSA moduli with primes of the same size for which our reduction fails is bounded above by (using Theorem 2.1)

$$\left( \frac{\log \sqrt{x^2 - x}}{2} \right) = O \left( \frac{x}{\log^{3/2} x} \right),$$

and if we assume the GRH this upper bound can be strengthened to $O(x^{3/4})$. Thus, our reduction does indeed work on a density 1 subset of the “interesting” RSA moduli.

Remark 2.6. For CM-forms, the prime indexed Fourier coefficients vanish for, roughly, half the primes. And our reduction will fail if both the prime factors of $n$ are divisible by such primes.

2.1. Computing a basis of cusp forms. Theorem 2.2 has the following consequence for the problem of computing any basis of cusp forms (with algebraic Fourier coefficients) for $S_k(\Gamma_0(N), \chi)$.

Corollary 2.7. Fix $N$, a positive integer, $k \geq 2$, an even integer, and $\chi$ a Dirichlet character modulo $N$. Assume that $S_k(\Gamma_0(N), \chi)$ contains a Hecke eigenform of non-CM type. Fix also a basis given by the Fourier expansion

$$f_i = \sum_{1 \leq m \leq q^m} a_i(m)q^m \text{ for } 1 \leq i \leq d,$$

such that the $a_i(m)$’s are algebraic. Suppose there is a polynomial time algorithm that, given $n$, computes the list of Fourier coefficients, $a_i(m)$, for $1 \leq i \leq d$, then there is a polynomial time algorithm that can factor a density 1 subset of the RSA moduli.

Proof: By our assumption there is a Hecke eigenform not of CM-type in $S_k(\Gamma_0(N), \chi)$. This form can be normalized by taking a scalar multiple, call this normalized eigenform $g$. Now, since $g$ belongs to $S_k(\Gamma_0(N), \chi)$ and the $f_i$ span the space we must have that $g = \sum_{1 \leq i \leq d} \alpha_if_i$, where $\alpha_i$ are algebraic numbers. The $n$-th Fourier coefficient of $g$ is $\sum_{1 \leq i \leq d} \alpha_i a_i(m)$, and so this can be computed (in polynomial time) using the supposed algorithm for computing the $a_i(m)$’s. The result now follows from Theorem 2.2. \qed

We now investigate the conditions under which the assumption made in Corollary 2.7 (that $S_k(\Gamma_0(N), \chi)$ contains an eigenform of non-CM type) holds. A construction due to Hecke (Hec37, also described by Shimura) shows how one can obtain essentially all the eigenforms of CM-type (see Rib77 §3). This construction together with dimension formulas for $S_k(\Gamma_0(N), \chi)$ can be used to show the existence of eigenforms of non-CM type. The results of Theorem 3.5 and Corollary 3.5 of Rib77 summarize the construction of CM forms by Hecke. Essentially, these results imply that one gets CM-forms corresponding to quadratic imaginary fields of discriminant $D$ dividing the level $N$, and each ideal class character of the orders of discriminant $N$ in these fields. From this observation and bounds on class numbers of imaginary quadratic fields, we find that the number of eigenforms of CM-type in $S_k(\Gamma_0(N), \chi)$ is bounded above by $N^{\frac{1}{2} + \epsilon}$ for every $\epsilon > 0$. The dimension of $S_k(\Gamma_0(N), \chi)$ (see [CO77]) on the other hand is $\Omega(kN)$. Furthermore, the space $S_k(\Gamma_0(N), \chi)$ has a basis of eigenforms; thus, if $N$ and $k$ are large enough there will always be eigenforms in $S_k(\Gamma_0(N), \chi)$ that are not of CM-type. In other words, for large enough $k$ and $N$, the assumption made in Corollary 2.7 holds. Consequently, computing a basis for such spaces is at least as hard as factoring RSA moduli.
2.2. The Ramanujan Tau function. The Ramanujan Tau function $\tau(n)$ is defined to be the $n$-th Fourier coefficient of the Discriminant function $\Delta(z)$:

$$\Delta(z) = q \prod_{1 \leq n} (1-q^n)^{24},$$

$$= 1 - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 + \cdots$$

$$= \sum_{1 \leq n} \tau(n)q^n.$$

It is a fact that $\Delta$ is a Hecke eigenform of weight 12 and level 1. There are no CM forms of level 1 (since the discriminant of the underlying CM field must divide the level), so $\Delta$ is not a CM form. Moreover, a conjecture of Lehmer states that $\tau(n)$ is never zero. If we assume Lehmer’s conjecture then the proof of our result now yields a slightly stronger conclusion:

**Corollary 2.8.** Assuming Lehmer’s conjecture, computing the Ramanujan tau function is at least as hard as factoring RSA moduli.

**Acknowledgement:** The authors would like to thank Tonghai Yang for pointing them to Hecke’s construction of CM forms.

**References**

[BC03] W. Bosma and J. Cannon. Handbook of MAGMA Functions. Sydney, 2003.

[BMS86] E. Bach, G. Miller, and J. Shallit. Sums of divisors, perfect numbers, and factoring. SIAM Journal on Computing, 15:1143–1154, 1986.

[Cha05] D. Charles. *Computational aspects of Modular Forms and Elliptic Curves*. PhD thesis, University of Wisconsin-Madison, 2005.

[Cha06] D. Charles. Computing the Ramanujan Tau function. Ramanujan Journal, 11(2):221–224, 2006.

[CO77] H. Cohen and J. Oesterlé. Dimensions des espaces de formes modulaires. Springer Lecture Notes in Mathematics, 627:69–78, 1977.

[DS05] F. Diamond and J. Shurman. *A first course in Modular Forms*. 2nd edition, 2005.

[ECDJ+06] B. Edixhoven, J.-M. Couveignes, R. de Jong, F. Merkl, and J. Bosman. On the computation of coefficients of a modular form. arXiv:math.NT/0605244, 2006.

[Gou97] E. Gouvêa. Non-ordinary primes: A story. *Experiment. Math.*, 6:195–205, 1997.

[Hec37] E. Hecke. Über Dirichlet-reihen mit funktionalgleichung und ihre nullstellen auf der mittelgeraden. Sitzungsberichte der Bayerischen Akademie der Wissenschaften. Mathematisch-naturwissenschaftliche Abteilung, pages 73–95, 1937.

[Kob93] N. Kobliizt. Introduction to Elliptic Curves and Modular Forms, volume 97 of Graduate Texts in Mathematics. Springer-Verlag, 2nd edition, 1993.

[Lan76] S. Lang. *Introduction to Modular Forms*, volume 222 of Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1976.

[Leh43] D. H. Lehmer. Ramanujan’s function $\tau(n)$. Duke Math. J., 10:483–492, 1943.

[Mer94] L. Merel. Universal Fourier expansions of modular forms. In *On Artin’s Conjecture for odd 2-dimensional representations*, volume 1585 of Springer Lecture Notes in Mathematics. Springer-Verlag, 1994.

[Ono04] K. Ono. *The Web of Modularity: Arithmetic of Coefficients of Modular Forms and q-Series*, volume 102 of CBMS Regional Conference Series in Mathematics. American Mathematical Society, 2004.

[Piz80] A. Pizer. An algorithm for computing modular forms on $\Gamma_0(N)$. Journal of Algebra, 64:340–390, 1980.

[Rib77] K. Ribet. Galois representations attached to Eigenforms with Nebentypus, volume 601 of Springer Lecture Notes in Mathematics, pages 17–52. Springer-Verlag, 1977.

[Sch85] R. Schoof. Elliptic curves over finite fields and computation of square roots mod $p$. *Math. Comp.*, 44:483–494, 1985.

[Ser70] J.-P. Serre. *A Course in Arithmetic*, volume 7 of Graduate Texts in Mathematics. Springer-Verlag, 1970.

[Ser81] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. Publ. Math. I.H.E.S., 54:123–201, 1981.

[Shi71] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, 1971.

[Ste00] W. Stein. *Explicit approaches to Modular Abelian Varieties*. PhD thesis, University of California, Berkeley, 2000.

**E-mail address:** bach@cs.wisc.edu

**Microsoft Research, One Microsoft Way, Redmond, WA - 98052**

**E-mail address:** cdx@microsoft.com