

Computationally  
Feasible Bounds for  
Quadratic Forms and  
CM Lifts of  
Supersingular Elliptic  
Curves

Ben Kane

November 30, 2007

B. Kane, Representations of Integers by Ternary Quadratic Forms, submitted for publication.

B. Kane, CM liftings of Supersingular Elliptic Curves, submitted for publication.

Let  $Q$  be a positive definite integral quadratic form in  $m$  variables and let

$$\theta_Q(\tau) := \sum_{x \in \mathbb{Z}^m} q^{Q(x)} = \sum_{n=1}^{\infty} r_Q(n) q^n$$

be the associated theta series, where  $q = e(\tau) = e^{2\pi i \tau}$  and  $r_Q(n)$  is the number of representations of  $n$  by  $Q$ .

$\theta$  is a modular form of weight  $\frac{m}{2}$ .

Example:

$$Q(x, y, z) := x^2 + 3y^2 + 5z^2 + 2yz$$

Question: Which positive integers  $n$  are represented by  $Q$ ?

Studied by a myriad of authors.

1. Gauss
2. Lagrange - "Four Squares Theorem"
3. Legendre - Three Squares (Leads to Study of Regular/Irregular Forms)
4. Bhargava - "15 Theorem" (Originally Conway -Schneeberger) and "290 Theorem" (with Hanke)

Local conditions show that some  $n$  cannot be represented.

**Definition 1.** *Eligible Integers* are those integers which are locally represented.

### **Regular and Irregular forms**

**Definition 2.** *Regular Quadratic Forms* are forms which represent every eligible integer.

Irregular forms do not represent every eligible integer.

Noting  $\theta$  is a modular form, get decomposition

$$\theta = E + g, \quad (1)$$

where  $E$  is the Eisenstein series and  $g$  is a cusp form.

Recalling definition of  $\theta$ , the  $n$ -th Fourier coefficient,  $a_\theta(n)$ , determines number of times  $Q$  represents  $n$ .

Decomposition gives

$$a_\theta(n) = a_E(n) + a_g(n) \quad (2)$$

## Basic Argument

- Study Asymptotics for  $a_E(n)$ ,  $a_g(n)$
- Show  $a_E(n) \gg a_g(n)$
- Note  $a_E(n) > 0$  here always.

Using trivial bounds, Tartakowsky (1928) showed for  $m \geq 5$ , every sufficiently large eligible integer is represented.

Subconvexity bounds of Kloosterman, and later Deligne's amazing optimal bound for integer weight cusp forms show  $m = 4$  case.

We study here  $m = 3$ .

Complications:

I Anisotropic primes

II Coefficients  $a_E(n)$  grow like Class Number.

III Trivial bounds insufficient! Need Subconvexity for non-integer weight cusp forms

IV Spinor Genus (won't talk about here – Doesn't come up in case we're interested in)

## I. Anisotropic Primes

**Definition 3.** Anisotropic primes are primes  $p$  such that

$$a_E(np^{2r}) = a_E(np^{2r+2})$$

for  $r$  sufficiently large.

So  $a_E(n)$  doesn't grow with high divisibility by  $p$ .

Anisotropic primes determined by local conditions.

## II. Class Numbers

Siegel showed Class Numbers grow like  $n^{\frac{1}{2} \pm \epsilon}$ .

Results were ineffective! Showed it assuming Riemann Hypothesis, then showed it by assuming the Riemann Hypothesis was false.

Littlewood showed GRH for Dirichlet  $L$ - functions gives effective bound.

### III. Weight $3/2$ subconvexity

Duke shows wonderful subconvexity result!

**Theorem 1** (Duke). *For  $g \in S_{3/2}(\Gamma)$ ,*

$$a_g(n) \ll n^{3/7+\epsilon} \quad (3)$$

Therefore, every sufficiently large eligible integer is represented!

Problems:

- 1) Ineffective result for  $a_E(n)$ .
- 2) Constant Effective for subconvexity, but not explicit.
- 3) Even assuming GRH for Dirichlet  $L$ -functions, bound obtained not computationally feasible (very, very large).

Ono and Soundararajan observe that additional assumption of GRH for weight 2 modular forms gives feasible bound for Ramanujan's Ternary Form  $Q = x^2 + y^2 + 10z^2$ .

With the help of a computer, they show

**Theorem 2** (Ono-Soundararajan). *Assuming GRH for Dirichlet  $L$ -functions and weight 2 modular forms, the only eligible integers not represented by  $Q$  are exactly*

3, 7, 21, 31, 33, 43, 67, 79, 87, 133, 217, 219, 223,  
253, 307, 391, 679, 2719.

## Connection to Elliptic Curves

Want to study whether or not a supersingular Elliptic Curve lifts to a CM Elliptic Curve.

1. Take  $E/\overline{\mathbb{F}}_p$  Supersingular
2. Endomorphisms are maximal order  $\mathcal{O}$  of Quaternion Algebra ramified exactly at  $p$  and  $\infty$ .
3. Deuring Lift shows that  $E$  lifts to an elliptic curve over a number field with CM by  $\mathcal{O}_{-D}$  if and only if  $\mathcal{O}_{-D}$  embeds optimally in  $\mathcal{O}$ .
4. Gross showed that  $\mathcal{O}_{-D}$  embeds optimally if and only if the norm on  $(2\mathcal{O} + \mathbb{Z})^0$  (the trace zero elements) represents  $D$ . Moreover, Gross shows the norm is a quadratic

form  $Q$  with  $\theta_Q \in M_{3/2}^+(4p)$  (Kohnen's plus space).

5. For  $K$  a number field,  $\mathbb{F}_q$  a finite field, and  $\pi$  the reduction map.  $E'$  CM by  $\mathcal{O}_{-D}$  and  $E$  supersingular by maximal order  $M$ .

Curve $C$	$End(C)$	
$E'/K$	$\mathcal{O}_{-D}$	$\rightarrow (2\mathcal{O}_{-D} + \mathbb{Z})^0$
$\updownarrow \pi ?$	$\downarrow$	$\downarrow \text{NORM}$
$E/\mathbb{F}_q$	$M$	$\rightarrow (2M + \mathbb{Z})^0$
		$\uparrow \text{NORM}$
		$\uparrow D$

## The Goal

1. Generalize Ono and Soundararajan's work to include  $\theta \in M_{3/2}^+(4p)$ .
2. Use Connection to Deuring Lifts to determine whether  $E$  Supersingular Elliptic Curve lifts to an Elliptic Curve over a Number Field with CM by  $\mathcal{O}_{-D}$ .
3. Write Algorithm to explicitly compute constants (Assuming GRH for Dirichlet  $L$ - functions and weight 2 modular forms)
4. Implement Algorithm, and, in computationally feasible cases, list all  $D$  which the curve does not lift to.

## The Results

**Theorem 3** (K.). *Let a prime  $p$  be given with  $\theta \in M_{3/2}^+(4p)$ . Assume GRH for Dirichlet  $L$ -functions and  $L$ -functions of weight 2 newforms in  $S_2(p)$ .*

*Then there exists an (explicit) algorithm to compute a constant  $D_\theta$  such that for every eligible fundamental discriminant  $-D$  with  $D > D_\theta$ ,  $a_\theta(D) \neq 0$ .*

*Moreover, for small  $p$  this bound is “computationally feasible”, so that we obtain a feasible algorithm to determine the complete set of eligible fundamental discriminants  $-D$  such that  $a_\theta(D) = 0$ .*

Use Hecke Operators and Shimura Correspondence to deal with non-fundamental discriminants.

**Definition 4.** The  $D$ -th Shimura correspondence  $G_D \in S_2(2p)$  of  $g$  satisfies

$$\sum_n \frac{a_{G_D}(n)}{n^s} := L(s, \chi_{-D}) \sum_{n=1}^{\infty} \frac{a_g(Dn^2)}{n^s}.$$

**Definition 5.** Hecke operator  $T_{l^2}$  defined via  $g|T_{l^2} = h$  with

$$\begin{aligned} a_h(d) = & a_g(l^2d) + \chi(l) \left( \frac{(-1)^k}{l} \right) l^{k-1} a_g(d) \\ & + \chi(l^2) \left( \frac{(-1)^k}{l^2} \right) l^{2k-1} a_g\left(\frac{d}{l^2}\right). \end{aligned} \quad (4)$$

**Theorem 4.** Fix a discriminant  $-d$ . If  $a_\theta(dF^2) = 0$  with  $(F, p) = 1$ , then

$$F \ll_\epsilon (p-1)^{2+\epsilon} \left( \sum_{i=1}^m |b_i| \right)^{2+\epsilon} d^{\frac{6}{7}+\epsilon}. \quad (5)$$

If we further assume the Riemann Hypothesis for Dirichlet  $L$ -functions, then

$$F \ll_\epsilon (p-1)^{2+\epsilon} \left( \sum_{i=1}^m |b_i| \right)^{2+\epsilon} d^{-\frac{1}{7}+\epsilon}. \quad (6)$$

Finally, if we additionally assume the Riemann Hypothesis for  $L$ -functions of weight 2 modular forms, then

$$F \ll_\epsilon (p-1)^{2+\epsilon} \left( \sum_{i=1}^m |b_i| \right)^{2+\epsilon} d^{-\frac{1}{2}+\epsilon}. \quad (7)$$

Here the assumed constants are effectively computable.

Using a technique of Duke, dependence on  $\theta$  can be removed.

Lose computational feasibility, but get growth in terms of  $p$ .

**Theorem 5** (K.). *Let  $p$  be a prime,  $\theta \in M_{3/2}^+(4p)$ , and  $\epsilon > 0$ . Assuming GRH for Dirichlet  $L$ -functions and weight 2 modular forms,  $a_\theta(d) \neq 0$  for every discriminant  $-d$  with  $\left(\frac{-d}{p}\right) \neq 1$  and  $p^2 \nmid d$  such that*

$$d \gg_\epsilon p^{12+\epsilon}.$$

*Here the assumed constant depends only on  $\epsilon$  and is effective.*

Side Note: An explicit constant for the optimal Ramanujan-Petersson bound for weight  $3/2$  cusp forms, conditional upon GRH for weight 2 cusp forms, is obtained as a side effect of the proof of Theorem 3.

**Corollary 1** (K.). Let  $N$  be squarefree and odd,  $\delta > 0$ , and  $g \in S_{3/2}^+(4N)$ . Assuming GRH for weight 2 modular forms, there is an effectively computable constant  $c_{g,\delta}$  such that

$$|a_g(n)| \leq c_{g,\delta} n^{\frac{1}{4} + \delta}.$$

Setting  $\delta = \epsilon$  gives optimal bound, but constant impractical. In practice, better choice here makes algorithm feasible. Explicit algorithm given.

## Feasible Cases

Computations show the following.

**Theorem 6** (K.). *Assume GRH for Dirichlet  $L$ -functions and weight 2 modular forms. Consider  $d$  such that  $11^2 \nmid d$  and  $\left(\frac{-d}{11}\right) \neq 1$ . Then*

1.  $Q(x, y, z) = 4x^2 + 11y^2 + 12z^2 + 4xz$  represents  $d$  if and only if

$$d \notin \{3, 67, 235, 427\}. \quad (8)$$

2.  $Q(x, y, z) = 3x^2 + 15y^2 + 15z^2 - 2xy + 2xz + 14yz$  represents  $d$  if and only if

$$d \notin \{4, 11, 88, 91, 163, 187, 232, 499, 595, 627, 715, 907, 1387, 1411, 3003, 3355, 4411, 5107, 6787, 10483, 11803\} \quad (9)$$

3. Moreover, these are a full set of representatives for  $Q$  such that  $\theta \in M_{3/2}^+(44)$ .
4. If  $-d = -D$  is a fundamental discriminant other than the 25 listed above, then every supersingular elliptic curve over  $\overline{\mathbb{F}}_{11}$  can be lifted to an elliptic curve over a number field with CM by  $\mathcal{O}_{-D}$ .

**Theorem 7.** *Assume GRH for Dirichlet  $L$ -functions and  $L$ -functions of weight 2 newforms. Consider  $d$  such that  $17^2 \nmid d$  and  $\left(\frac{-d}{17}\right) \neq 1$ . Then*

1.  $Q(x, y, z) = 7x^2 + 11y^2 + 20z^2 - 6xy + 4xz + 8yz$  represents  $d$  if and only if

$$d \notin \{3, 187, 643\}, \quad (10)$$

and  $Q$  represents  $d$  if and only if  $Q$  represents  $d(17)^2$ .

2.  $Q(x, y, z) = 3x^2 + 23y^2 + 23z^2 - 2xy + 2xz + 22yz$  represents  $d$  if and only if

$$d \notin T$$

where  $\#T = 88$ , the largest element of  $T$  is 89563, and  $Q$  represents  $d$  if and only if  $Q$  represents  $d(17)^2$ .

3. Moreover, these are a full set of representatives for  $Q$  such that  $\theta \in M_{3/2}^+(68)$ .

4. If  $-d = -D$  is a fundamental discriminant other than the 91 elements above, then every supersingular elliptic curve over  $\overline{\mathbb{F}}_{17}$  can be lifted to an elliptic curve over a number field, with CM by  $\mathcal{O}_{-D}$ .

The case  $p = 19$  has also been fully computed.

**Theorem 8** (K.). *Assume GRH for Dirichlet  $L$ -functions and weight 2 modular forms. Consider  $d$  such that  $19^2 \nmid d$  and  $\left(\frac{-d}{19}\right) \neq 1$ . Then*

1.  $Q(x, y, z) = 7x^2 + 11y^2 + 23z^2 - 2xy + 6xz + 10yz$  represents  $d$  if and only if

$$d \notin \{4, 19, 163, 760, 1051\}. \quad (11)$$

2. The set of  $d$  which  $Q(x, y, z) = 4x^2 + 19y^2 + 20z^2 + 4xz$  does not represent has size 40, and the largest such is  $d = 27955$ .

3. Moreover, these are a full set of representatives for  $Q$  such that  $\theta \in M_{3/2}^+(76)$ .

4. If  $-d = -D$  is a fundamental discriminant other than the 45 above (in particular if  $D > 27955$ ), then every supersingular elliptic curve over  $\overline{\mathbb{F}}_{19}$  lifts to an elliptic curve over a number field, with CM by  $\mathcal{O}_{-D}$ .

Explicit computation of the bound from Theorem 3 shows the following for  $p \leq 107$ .

**Theorem 9** (K.). *Assume GRH for weight 2 modular forms and Dirichlet  $L$ -functions. Fix  $p \leq 107$ . Every  $E/\overline{\mathbb{F}}_p$  lifts to an elliptic curve with CM by  $\mathcal{O}_{-D}$  for every  $D > 4 \times 10^{25}$ , up to local conditions.*

## Basic Overview for Proof of Theorem 3

1. Decompose  $\theta$  further:

$$\theta = E + \sum_{i=1}^r b_i g_i, \quad (12)$$

where  $g_i$  are fixed Hecke eigenforms.

2. Use variant of Kohnen-Zagier Formula to show

$$|a_{g_i}(D)|^2 = c_i 2^{-v_p(D)} D^{\frac{1}{2}} \cdot L_i(1) \quad (13)$$

with  $c_i$  an explicit constant and

$$L_i(s) := L(G_i, -D, s) := \sum_{n=1}^{\infty} \frac{\chi(n) a_{G_i}(D)}{n^s}. \quad (14)$$

is the  $L$  series of  $G_i$  twisted by the character  $\chi = \chi_{-D}$ .

3. Gross shows explicit formula

$$a_E(D) = \frac{12}{(p-1)} \frac{H(-D)}{2^{v_p(D)}} \quad (15)$$

4. Use Dirichlet's Class Number Formula

$$h(-D) = \frac{L(1)\sqrt{D}}{\pi}. \quad (16)$$

with  $L(s) := L(s, \chi)$ .

5. Combining (12), (13), (15), (16), Schwartz inequality gives (for  $D > 4$ )

$$\frac{12}{(p-1)\pi 2^{\frac{v_p(D)}{2}}} \cdot D^{\frac{1}{4}} \leq \sqrt{\sum_{i=1}^r |b_i|^2} \sqrt{\sum_{i=1}^r c_i \frac{L_i(1)}{L(1)^2}}. \quad (17)$$

6. Now we bound  $\frac{L_i(1)}{L(1)^2}$ . Define

$$F(s) := F_i(s) := \left(\frac{\sqrt{q}}{2\pi}\right)^{s-1} \frac{L_i(s)\Gamma(s)}{L(s)L(2-s)}, \quad (18)$$

where  $q$  is the conductor of  $L_i$ .

7. Assume GRH for Dirichlet  $L$ -functions.  $F(s)$  holomorphic for  $\frac{1}{2} < \sigma = \operatorname{Re}(s) < \frac{3}{2}$ . Functional equation of  $L(s)$  gives

$$F(s) = F(2-s)$$

Phragmen-Lindelöf shows max at boundary,  $\operatorname{Re}(s) = \sigma$  for  $1 < \sigma < \frac{3}{2}$ . Thus

$$F(1) \leq \max_t |F(\sigma + it)|. \quad (19)$$

8. Use Hadamard's Exact formulas for  $\frac{L'}{L}(s)$  and  $\frac{L'_i}{L_i}(s)$ .
9. Integrate both sides of formula and take real parts.
10. Bound terms coming from  $L(s)$  from below, and  $L_i(s)$  from above. Uses bounds for  $\frac{\Gamma'}{\Gamma}$  often.
11. Bounds depend heavily on locations of zeros of  $L(s)$  and  $L_i(s)$ . GRH for Dirichlet  $L$ -functions gives zeros of  $L(s)$  at  $\sigma = \frac{1}{2}$ . GRH for weight 2 modular forms implies zeros of  $L_i(s)$  at  $\sigma = 1$ .

12. Asymptotically better bounds for  $\sigma \rightarrow 1$ , but constant grows very large.
13. Fixing form  $Q$ , get more feasible bounds for better choices of  $\sigma$ .