Class Numbers and Exponential Sums

Lillian B. Pierce
University of Oxford
lillian.pierce@maths.ox.ac.uk

Exponential Sums over Finite Fields and Applications

1-5 November 2010 ETH Zürich

An introduction to class numbers

$\mathbb{Z}$ has unique factorization:

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

O_K for $K = \mathbb{Q}(\sqrt{-5})$ does not:

$$21 = 3 \cdot 7 \qquad\qquad 21 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5})$$

General setting:
Number field $K/\mathbb{Q}$
Class Group $CL(K)$

$$CL(K) = I_K/K^* = \text{fractional ideals/principal fractional ideals}$$

Class number $h(K)$

$$h(K) = |CL(K)|$$

Properties:

- $h(K)$ is finite
- $h(K) = 1$ implies unique factorization

Questions:

- growth
- divisibility

Why would we care?

The shortest (false) proof of FLT: $x^p + y^p = z^p$

$$y^p = z^p - x^p \iff y \cdot y \cdots y = (z - x)(z - \mu x) \cdots (z - \mu^{p-1} x)$$

Dirichlet's class number formula:

$$\mathrm{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1} (2\pi)^{r_2} R_K}{\omega_K \sqrt{|D_K|}} h(K)$$

Class numbers of quadratic fields: growth

- quadratic field $\mathbb{Q}(\sqrt{d})$
- class group $CL(d)$
- class number $h(d)$

Imaginary fields $\mathbb{Q}(\sqrt{-d})$, $d > 0$

Theorem (Gauss Class Number Conjecture)

Given a positive integer h,

$$h(-d) = h$$

for finitely many square-free $-d < 0$.

Real fields $\mathbb{Q}(\sqrt{d})$**,** $d > 0$

Conjecture

$h(d) = 1$ *for infinitely many* $d > 0$.

Class numbers of quadratic fields: divisibility

Define

$$\mathcal{N}_g^-(X) = \#\{-X \leq d < 0,\ d \text{ square-free:} \exists\ [\mathfrak{a}] \in CL(d),\ [\mathfrak{a}]^g = I\}$$

Define $\mathcal{N}_g^+(X)$ equivalently for real fields, $0 < d \leq X$.
Gauss Genus Theory (1801)

$$\mathcal{N}_2^{\pm}(X) \sim \frac{6}{\pi^2} X$$

Conjecture (Cohen-Lenstra heuristics, 1984)
For each integer $g \geq 3$,

$$\mathcal{N}_g^-(X) \sim C_g^- X \quad \textit{and} \quad \mathcal{N}_g^+(X) \sim C_g^+ X$$

for **explicit** *constants C_g^- (imaginary case) and C_g^+ (real case).*

Our focus: the 3-part of the class number

Definition: the 3-part of the class number (d pos. or neg.)

$$h_3(d) = \#\{[\mathfrak{a}] \in CL(d) : [\mathfrak{a}]^3 = I\}$$

Trivial bound:

$$h_3(d) \leq h(d) \ll |d|^{1/2+\epsilon}$$

Conjecture: For any $\epsilon > 0$,

$$h_3(d) \ll |d|^{\epsilon}$$

Prix Fixe Menu for today:

- Part I: averages of $h_3(d)$
- Part II: individual bounds for $h_3(d)$

Part I: Averages of the 3-part

We'd like to understand

$$\sum_{0<d<X} h_3(d), \qquad \sum_{-X<d<0} h_3(d).$$

Consider a fundamental discriminant d, and set

$$H(d) = \frac{h_3(d) - 1}{2}$$

Properties

- $H(d) \geq 0$
- $H(d) = 0 \iff 3 \nmid h(d)$
- Hasse: $H(d) =$ the number of triplets of cubic fields of discriminant d in which no prime ramifies completely

Davenport-Heilbronn correspondence

$$\begin{array}{ccc} \text{triplets of such cubic fields} & & \text{equivalence classes under } GL_2(\mathbb{Z}) \\ \text{of discriminant } d & \longleftrightarrow & \text{of irred binary cubic} \\ & & \text{forms of disc } d \end{array}$$

Counting binary cubic forms

Binary cubic form $F(x, y)$, identified with $(a, b, c, d) \in \mathbb{R}^4$:

$$aX^3 + bX^2Y + cXY^2 + dY^3$$

Discriminant

- $\Delta(a, b, c, d) = b^2c^2 + 18abcd - 27a^2d^2 - 4b^3d - 4c^3a$
- homogeneous form of degree 4 in 4 variables

Another correspondence:

binary cubic form $\longleftrightarrow$ positive definite binary quadratic form

Example: For $\Delta > 0$, we may take $Q = \text{Hessian}(F)$,

$$Q(x, y) = Ax^2 + Bxy + Cy^2,$$

where $\quad A = b^2 - 3ac, \quad B = bc - 9ad, \quad C = c^2 - 3bd.$

Applying the correspondence

Define the domain

$$\mathcal{V}_0 = \{(a,b,c,d) \in \mathbb{R}^4 : a \geq 1 \text{ and either } -A < B \leq A < C \\ \text{or } 0 \leq B \leq A = C\}$$

Then $\mathcal{V}_0$ contains a "canonical" representative of each $GL_2(\mathbb{Z})$ equivalence class of binary cubic forms.

New description of $H(d)$:

For any *positive* fundamental discriminant d,

$$H(d) = \frac{1}{2}\#\{(a,b,c,d) \in \mathcal{V}_0 : aX^3 + bX^2Y + cXY^2 + dY^3 \text{ is irred.} \\ \text{and } \Delta(a,b,c,d) = d\}$$

Davenport and Heilbronn (1971)

Set $\alpha^+ = 1$, $\alpha^- = 3$. Then

$$\sum_{d \in \Delta^\pm(X)} H(d) \sim \frac{\alpha^\pm}{6} \sum_{d \in \Delta^\pm(X)} 1 \sim \alpha^\pm \frac{X}{2\pi^2}$$

Further results of Davenport-Heilbronn correspondence

Belabas (1996)
For q square-free, $q \leq X^{1/15-\epsilon}$, as $X \to \infty$,

$$\sum_{\substack{d \in \Delta^{\pm}(X) \\ d \equiv 0 \pmod{q}}} H(d) \sim \frac{\alpha^{\pm}}{2\pi^2} \frac{\nu(q)}{q} X.$$

Here $\nu(p) = p/(p+1)$ defines ν multiplicatively.

Fouvry (1999), Fouvry and Katz (2001)
There exists $c_0 > 0$ and x_0 such that for $x > x_0$,

$$\#\{p \leq x : p \equiv 1 \pmod{4}, p{+}4 \text{ square-free}, 3 \nmid h(p{+}4)\} \geq c_0 \frac{x}{\log x}$$

Moments, convolutions, and twisted averages

We'd like to understand

$$\sum_{0<d\le X} (h_3(d))^2, \qquad \sum_{0<d\le X} h_3(d)h_3(d+r)$$

First step is to understand

$$\sum_{0<d\le X} h_3(d)e_q(\alpha d), \qquad \text{with } (\alpha, q) = 1$$

Simplification: Enlarge $\mathcal{V}_0$ to $\mathcal{V}$, where

$$\mathcal{V} = \{(a, b, c, d) \in \mathbb{R}^4 : a \ge 1, |B| \le A \le C\}$$

Define for every $n \ge 1$:

$$g(n) = \#\{(a, b, c, d) \in \mathcal{V} : \Delta(a, b, c, d) = n\}.$$

Then $H(n) = \frac{1}{2}(h_3(n) - 1) \le \frac{1}{2}g(n)$.

A twisted average

Goal is to bound

$$\sum_{0<n\leq X} g(n)e_q(\alpha n), \qquad \text{for fixed } (\alpha, q) = 1$$

We want to count points in the region

$$\mathcal{V}(X) = \{(a,b,c,d) \in \mathbb{R}^4 : a \geq 1, |B| \leq A \leq C, 0 < \Delta(a,b,c,d) \leq X\}$$

- truncate to remove cusp, $a \ll X^{1/4-3\eta}$ (any fixed small $\eta > 0$)
- decompose into XQ^{-4} hypercubes of side length Q

$$\mathcal{V} = \left(\bigcup \text{boxes}\right) \cup \text{margins} \cup \text{cusp} = \left(\bigcup \mathcal{B}_i\right) \cup \mathcal{D} \cup \mathcal{E}$$

Lemma (Davenport, Belabas and Fouvry)

$$\begin{aligned} |\mathcal{E}| &= O(X^{1-\eta}) \\ |\mathcal{D}| &= O(X^{1-\eta} + QX^{3/4+3\eta}\log X + Q^3X^{1/4} + Q^4) \\ &= O(X^{1-\eta}), \qquad \text{with the choice } Q = X^{1/4-4\eta}(\log X)^{-1} \end{aligned}$$

Compute average for each box (case with $Q \leq q$)

Compute the twisted average for each box $\mathcal{B}$:

$$T(\mathcal{B}) = \sum_{0<n\leq X} \sum_{\substack{\mathbf{x}\in\mathcal{B} \\ \Delta(\mathbf{x})=n}} e_q(\alpha n) = \sum_{\beta \pmod q} \sum_{\substack{\mathbf{x}\in\mathcal{B} \\ \Delta(\mathbf{x})\equiv\beta(q)}} e_q(\alpha\beta)$$

Extend to complete character sum:

$$T(\mathcal{B}) = \frac{1}{q^4} \sum_{\mathbf{h} \pmod q)^4} S(\alpha, \mathbf{h}; q) \sum_{\mathbf{x}\in\mathcal{B}} e_q(-\mathbf{h}\cdot\mathbf{x}),$$

where

$$\begin{aligned} S(\alpha, \mathbf{h}; q) &= \sum_{\beta \pmod q} \sum_{\substack{\mathbf{a} \pmod q)^4 \\ \Delta(\mathbf{a})\equiv\beta \pmod q}} e_q(\mathbf{h}\cdot\mathbf{a}) e_q(\alpha\beta) \\ &= \sum_{\mathbf{a} \pmod q)^4} e_q(\alpha\Delta(\mathbf{a}) + \mathbf{h}\cdot\mathbf{a}) \end{aligned}$$

Key exponential sum bound

$$S(\alpha, \mathbf{h}; p) = \sum_{\mathbf{a} \pmod{q}^4} e_q(\alpha\Delta(\mathbf{a}) + \mathbf{h} \cdot \mathbf{a})$$

Theorem (Fouvry-Katz 2001)

There exists a constant $C = C_\alpha$ and closed subschemes $X_j \subset \mathbb{A}^4_{\mathbb{Z}}$ of relative dimension $\leq 4 - j$, with $X_4 \subset \cdots \subset X_1 \subset \mathbb{A}^4_{\mathbb{Z}}$, such that:

- for $\mathbf{h} \notin X_1(\mathbb{F}_p)$ (dim 3),
$$|S(\alpha, \mathbf{h}; p)| \leq Cp^2$$
- for $\mathbf{h} \notin X_2(\mathbb{F}_p)$ (dim 2),
$$|S(\alpha, \mathbf{h}; p)| \leq Cp^{5/2}$$
- for $\mathbf{h} \notin X_3(\mathbb{F}_p)$ (dim 1),
$$|S(\alpha, \mathbf{h}; p)| \leq Cp^3$$
- for $\mathbf{h} \notin X_4(\mathbb{F}_p)$ (dim 0),
$$|S(\alpha, \mathbf{h}; p)| \leq Cp^{7/2}$$

Twisted average for a box $\mathcal{B}$

In conclusion, for q square-free:

$$
\begin{aligned}
T(\mathcal{B}) &= \sum_{0<n\leq X} \sum_{\substack{\mathbf{x}\in\mathcal{B} \\ \Delta(\mathbf{x})=n}} e_q(\alpha n) \\
&\leq \frac{1}{q^4} \sum_{\mathbf{h} \pmod{q}^4} |S(\alpha, \mathbf{h}; q)| \left| \sum_{\mathbf{x}\in\mathcal{B}} e_q(-\mathbf{h}\cdot\mathbf{x}) \right| \\
&\leq \frac{1}{q^2} C_\alpha^{\nu(q)} \sum_{\delta_3|\delta_2|\delta_1|q} \delta_1^{1/2}\delta_2^{1/2}\delta_3^{1/2} \\
&\qquad \cdot \sideset{}{^\#}\sum_{\mathbf{h} \pmod{q}^4} E(\frac{h_1}{q})E(\frac{h_2}{q})E(\frac{h_3}{q})E(\frac{h_4}{q})
\end{aligned}
$$

- $\sum^{\#}$ requires for all $p|\delta_i$, $\mathbf{h} \pmod{p} \in X_i(\mathbb{F}_p)$
- $E(t) = \min(Q, ||t||^{-1})$

Final step: sum over boxes and include cusp and margins:

$$\sum_{0<n\leq X} g(n)e_q(\alpha n) = \sum_{\mathcal{B}_i} T(\mathcal{B}_i) + O(|\mathcal{D}|) + O(|\mathcal{E}|)$$

Theorem (L^p)

For any $1 \leq q \leq X^{1/2-8\eta}$*,* q *square-free,* $(\alpha, q) = 1$*, and* $\epsilon > 0$ *arbitrarily small,*

$$\sum_{0<n\leq X} g(n)e_q(\alpha n) \ll_\epsilon [Xq^{-1/2} + q^2X^{16\eta} + X^{1-\eta}](\log X)^4 q^\epsilon.$$

The analogous result also holds for $-X \leq n < 0$*.*

Part II: individual bounds for $h_3(d)$

Trivial bound:

$$h_3(d) \le h(d) \ll |d|^{1/2+\epsilon}$$

Conjecture: For any $\epsilon > 0$,

$$h_3(d) \ll |d|^{\epsilon}$$

Theorem (Ellenberg, Helfgott, LP^3, Venkatesh^2)

The 3-part $h_3(d)$ of the class number of the quadratic field $\mathbb{Q}(\sqrt{d})$ admits a bound

$$h_3(d) \ll |d|^{\theta+\epsilon}$$

where $\theta < 1/2$, for any $\epsilon > 0$.

Consequences of a nontrivial bound $h_3(d) \ll |d|^{\theta+\epsilon}$

Cubic Fields (Hasse 1930)
The number of cubic fields over $\mathbb{Q}$ with discriminant d is

$$O(|d|^{\theta+\epsilon})$$

Elliptic Curves with Fixed Conductor
(Brumer and Silverman 1996, Helfgott and Venkatesh 2006)

$$\#\{\mathcal{E}/\mathbb{Q} : \mathrm{cond}(\mathcal{E}) = N\} = O(N^{\alpha\theta+\epsilon}),$$

where $\alpha = 0.5065...$

Divisibility (Davenport and Heilbronn 1971)

$$\mathcal{N}_3^{\pm}(X) \gg X^{1-\theta+\epsilon}$$

Class group exponents (Heath-Brown 2008)

Reducing the problem to counting points

Reflection principle (Scholz 1932)

$$\log_3(h_3(-3d)) \le \log_3(h_3(+d)) \le \log_3(h_3(-3d)) + 1$$

Imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ with discriminant Δ
Suppose $[\mathfrak{a}] \in CL(-d)$, $[\mathfrak{a}]^3 = I$.
There is an integral ideal $\mathfrak{b} \in [\mathfrak{a}]$,

$$\mathfrak{N}(\mathfrak{b}) \le \frac{2}{\pi}\sqrt{|\Delta|}.$$

Furthermore, since $\mathfrak{b}^3$ is principal, we may write

$$4(\mathfrak{N}(\mathfrak{b}))^3 = y^2 + dz^2$$

for some $y, z \in \mathbb{N}$. Thus we have the upper bound:

$$h_3(-d) \le d^{\epsilon}\#\{4x^3 = y^2 + dz^2 : x \le d^{1/2}, y \le d^{3/4}, z \le d^{1/4}\}.$$

Similarly, for any $g \ge 3$,

$$h_g(-d) \le d^{\epsilon}\#\{4x^g = y^2 + dz^2 : x \le d^{1/2}, y \le d^{g/4}, z \le d^{g/4-1/2}\}.$$

Counting points on the surface $4x^3 = y^2 + dz^2$

Congruence (LP 2005)

$$4x^3 \equiv y^2 \pmod{d} \qquad\qquad \theta = 55/112$$

Square Sieve (LP 2006)

$$\boxed{y^2 = 4x^3 - dz^2 \qquad\qquad \theta = 27/56}$$

Elliptic Curve (Helfgott and Venkatesh 2006)

$$y^2 = 4x^3 + \delta \qquad\qquad \theta = 0.44178...$$

Congruence with divisibility (LP 2005)

$$4x^3 \equiv y^2 \pmod{d}, d_0 | d, d_0 \approx d^{5/6} \qquad\qquad \theta = 5/12$$

Symmetries (Ellenberg and Venkatesh 2007) $\qquad \theta = 1/3$

The square sieve: counting square values of a polynomial

Given:

- Polynomial $F(x_1, x_2, \ldots, x_k)$ with integer coefficients
- Box $\mathcal{B} = \prod_{i=1}^{k}[-B_i, B_i]$

Define:

- square counting function

$$N_{\mathcal{B}}(F) = \#\{\mathbf{x} \in \mathcal{B} : F(\mathbf{x}) = \square\}$$

- sieving function

$$\omega(n) = \#\{\mathbf{x} \in \mathcal{B} : F(\mathbf{x}) = n\}$$

The Square Sieve (Hooley 1978; Heath-Brown 1984)
Let $\mathcal{P}$ be a set of P primes. Suppose $\omega(n) = 0$ for $n = 0$ and for $|n| \geq e^P$. Then

$$N_{\mathcal{B}}(F) = \sum_n \omega(n^2) \ll P^{-1} \sum_n \omega(n) + P^{-2} \sum_{p \neq q \in \mathcal{P}} \left| \sum_n \omega(n) \left(\frac{n}{pq} \right) \right|.$$

Main sieve term

Sieving set for a parameter $Q \geq 1$:

$$\mathcal{P} = \{p \text{ prime} : Q \leq p \leq 2Q, p \text{ not ``bad'' for } F\}$$

Trivial leading term is bounded by

$$P^{-1} \sum_{n} \omega(n) \ll Q^{-1+\epsilon} \prod B_i$$

Main sieve term

$$\sum_{n} \omega(n) \left(\frac{n}{pq}\right) = \sum_{\mathbf{x} \in \mathcal{B}} \left(\frac{F(\mathbf{x})}{pq}\right) = \sum_{\mathbf{a} \pmod{pq}^k} \left(\frac{F(\mathbf{a})}{pq}\right) \sum_{\substack{\mathbf{x} \in \mathcal{B} \\ \mathbf{x} \equiv \mathbf{a} \pmod{pq}^k}} 1$$

$$\leq \frac{1}{(pq)^k} \sum_{\mathbf{m} \pmod{pq}^k} S_F(\mathbf{m}; pq) \prod_{i=1}^{k} \min(B_i, ||m_i/pq||^{-1})$$

with mixed character sum

$$S_F(\mathbf{m}; pq) = \sum_{\mathbf{a} \pmod{pq}^k} \left(\frac{F(\mathbf{a})}{pq}\right) e_{pq}(\mathbf{m} \cdot \mathbf{a})$$

Key exponential sum estimate

Weil bound: for p prime and suitable F,

$$|S_F(\mathbf{m}; p)| \leq c_{F,k} p^{k/2}$$

Sufficient due to handy multiplicative property: for $(q_1, q_2) = 1$,

$$S_F(\mathbf{m}; q_1 q_2) = S_F(\mathbf{m}\bar{q}_2; q_1) S_F(\mathbf{m}\bar{q}_1; q_2).$$

Conclusion for main sieve term

$$\sum_n \omega(n) \left(\frac{n}{pq}\right) \ll \prod_{i=1}^{k} \left[B_i (pq)^{-1/2} + (pq)^{1/2+\epsilon}\right]$$

Final result

$$N_{\mathcal{B}}(F) \ll Q^{-1+\epsilon} \prod B_i + Q^{k+\epsilon} \ll (\prod B_i)^{1-\frac{1}{k+1}+\epsilon}$$

Application to $h_3(-d)$

Relevant polynomial

$$F(x,z) = 4x^3 - dz^2$$

Relevant box

$$\mathcal{B} = [-B_1, B_1] \times [-B_2, B_2], \qquad B_1 = d^{1/2},\ B_2 = d^{1/4}$$

Sieving function

$$\omega(n) = \#\{(x,z) \in \mathcal{B} : 4x^3 - dz^2 = n\}$$

Square sieve result

$$h_3(-d) \ll d^{\epsilon} \sum_n \omega(n^2) \ll Q^{-1+\epsilon} d^{3/4} + Q^{2+\epsilon} \ll d^{1/2+\epsilon}.$$

This is as bad as the trivial bound!

What went wrong: completing the exponential sum

For a multiplicative character χ modulo r:

$$\begin{aligned}
\sum_{x \le X} \chi_r(f(x)) &= \sum_{a \pmod r} \chi_r(f(a)) \sum_{\substack{x \le X \\ x \equiv a \pmod r}} 1 \\
&= \frac{1}{r} \sum_{m \pmod r} \sum_{a \pmod r} \chi_r(f(a)) e_r(ma) \sum_{x \le X} e_r(-mx) \\
&\ll Xr^{-1/2} + r^{1/2+\epsilon}
\end{aligned}$$

We've passed through the Fourier transform in the wrong direction, unless

$$X \gg \sqrt{\text{modulus}}$$

What is the modulus?

- modulus: $pq \approx Q^2$, so we need $B_i > Q$
- the square sieve can do no better than $Q^{-1+\epsilon} \prod_{i=1}^{k} B_i$
- non-negotiable lower bound for Q comes from application

New method: decompose $\mathcal{B}$ into "big" and "little" dimensions:

$$\begin{aligned} \mathcal{B} &= \mathcal{B}_{(1)} \times \mathcal{B}_{(2)}, \qquad && \mathcal{B}_{(j)} \text{ of dimension } k_j \\ B_{(1)} &= \prod_{B_i \geq Q} B_i && B_{(2)} = \prod_{B_i < Q} B_i \end{aligned}$$

A trivial modification of the square sieve gives:

$$N_{\mathcal{B}}(F) \ll B_{(1)} B_{(2)} Q^{-1+\epsilon} + B_{(2)} Q^{k_1+\epsilon} \ll B_{(1)}^{1-\frac{1}{k_1+1}+\epsilon} B_{(2)}^{1+\epsilon}.$$

Application to class number $h_3(-d)$: $B_{(1)} = d^{1/2}, B_{(2)} = d^{1/4}$

New approach: reduce the size of the modulus

The q-analogue of van der Corput's method:
Developed by Heath-Brown (1981) to reduce modulus in sum

$$\mathbf{S} = \sum_{A<n\leq B} e_q(f(n))$$

Suppose $q = q_0 q_1$.
Then

$$H\mathbf{S} = \sum_{h=1}^{H} \sum_{A-hq_1<n\leq B-hq_1} e_q(f(n+hq_1))$$

Apply Cauchy's inequality:

$$H^2|\mathbf{S}|^2 \leq (B-A+Hq_1) \sum_{|h|<H} (H-|h|) \sum_{n\in I_{h,q}} e_{q_0 q_1}(f(n+hq_1))\overline{e_{q_0 q_1}(f(n))}$$

The new effective modulus:

$$q_0 < q$$

The split square sieve (LP 2006)

Let $\mathcal{A} = \{uv : u \in \mathcal{U}, v \in \mathcal{V}\}$ where $\mathcal{U}$ and $\mathcal{V}$ are disjoint sets of primes. Let $A = \#\mathcal{A}$, $U = \#\mathcal{U}$, and $V = \#\mathcal{V}$. Suppose that $\omega(n) = 0$ for $n = 0$ and for $|n| \geq \exp(\min(U, V))$. Then

$$\sum_n \omega(n^2) \ll A^{-1} \sum_n \omega(n) + A^{-2} \sum_{\substack{uv \neq u'v' \in \mathcal{A} \\ (uv, u'v')=1}} \left| \sum_n \omega(n) \left(\frac{n}{uu'vv'} \right) \right|$$

$$+ VA^{-2} \sum_{u \neq u' \in \mathcal{U}} \left| \sum_n \omega(n) \left(\frac{n}{uu'} \right) \right| + A^{-2} |E(\mathcal{U})|$$

$$+ UA^{-2} \sum_{v \neq v' \in \mathcal{V}} \left| \sum_n \omega(n) \left(\frac{n}{vv'} \right) \right| + A^{-2} |E(\mathcal{V})|.$$

The error term $E(\mathcal{U})$ (and analogously $E(\mathcal{V})$) is defined by:

$$E(\mathcal{U}) = \sum_{v \in \mathcal{V}} \sum_{u \neq u' \in \mathcal{U}} \sum_{\substack{n \\ v | n}} \omega(n) \left(\frac{n}{uu'} \right).$$

The general idea of how to apply the split square sieve

- Square counting function $N_{\mathcal{B}}(F) = \#\{\mathbf{x} \in \mathcal{B} : F(\mathbf{x}) = \square\}$
- Sieving function $\omega(n) = \#\{\mathbf{x} \in \mathcal{B} : F(\mathbf{x}) = n\}$
- Sieving sets for some parameter $Q \geq 1$, $0 < \alpha < 1$:

$$\begin{aligned} \mathcal{U} &= \{\text{primes } u : Q^{\alpha} < u \leq 2Q^{\alpha}\} \quad \textit{“big” primes} \\ \mathcal{V} &= \{\text{primes } v : Q^{1-\alpha} < v \leq 2Q^{1-\alpha}\} \quad \textit{“small” primes} \\ \mathcal{A} &= \{uv : u \in \mathcal{U}, v \in \mathcal{V}\} \end{aligned}$$

Sieving set cardinality

$$A \gg Q(\log Q)^{-2}$$

The main trivial term is bounded by

$$Q^{-1+\epsilon} \prod B_i = Q^{-1+\epsilon} B_{(1)} B_{(2)}$$

where

$$B_{(1)} = \prod_{B_i \geq Q} B_i \qquad\qquad B_{(2)} = \prod_{B_i < Q} B_i$$

Main sieve term in split square sieve

Main sieve term has modulus $r_0 r_1 = (uu')(vv') = (\text{big})(\text{small})$

$$\sum_n \omega(n) \left(\frac{n}{r_0 r_1} \right) = \sum_{\mathbf{x}_{(1)} \in \mathcal{B}_{(1)}} \sum_{\mathbf{x}_{(2)} \in \mathcal{B}_{(2)}} \left(\frac{F(\mathbf{x})}{r_0 r_1} \right)$$

Procedure:

- extend sum over $\mathbf{x}_{(1)} \in \mathcal{B}_{(1)}$ into a complete sum modulo $r_0 r_1$
- use the q-analogue of van der Corput's method to reduce modulus of remaining sum to r_0
- now the ranges of $\mathbf{x}_{(2)} \in \mathcal{B}_{(2)}$ satisfy $B_i \geq \sqrt{\text{modulus}}$
- extend sum over $\mathbf{x}_{(2)} \in \mathcal{B}_{(2)}$ to complete character sums modulo r_0

The key exponential sum

Exponential sum $S_F(\mathbf{h}, \mathbf{l}, \mathbf{m}; p)$ in $2k_1 + k_2$ variables:

$$\sum_{\substack{\mathbf{a} \pmod{p})^{k_1} \\ \mathbf{b} \pmod{p})^{k_1}}} \sum_{\mathbf{c} \pmod{p})^{k_2}} \left(\frac{F(\mathbf{a}, \mathbf{c} + \mathbf{h}r_1)}{p}\right) \left(\frac{F(\mathbf{b}, \mathbf{c})}{p}\right) e_p(\mathbf{l}\cdot\mathbf{a} - \mathbf{l}\cdot\mathbf{b} + \mathbf{m}\cdot\mathbf{c}),$$

where $\mathbf{l} \in \mathbb{Z}^{k_1}$, $\mathbf{h}, \mathbf{m} \in \mathbb{Z}^{k_2}$.

Reasonable hope:

$$\text{Bound}(S_F): \qquad |S_F(\mathbf{h}, \mathbf{l}, \mathbf{m}; p)| \ll p^{k_1 + k_2/2} \prod_{i=1}^{k_2} (p, m_i, h_i)^{1/2}$$

General conditional result:

Assuming Bound(S_F), the split square sieve yields

$$N_{\mathcal{B}}(F) \ll B_{(1)}^{1-\frac{1}{\kappa}} B_{(2)}^{1-\frac{1}{2\kappa}}, \qquad \kappa = k_1 + k_2/3 + 1$$

Compare to: $N_{\mathcal{B}}(F) \ll B_{(1)}^{1-\frac{1}{k_1+1}} B_{(2)}$

Application to 3-part of class number $h_3(-d)$

- Relevant polynomial $F(x,z) = 4x^3 - dz^2$
- Relevant modulus: $Q = d^{1/4+\delta}$, ultimately with $\delta = 1/56$
- Relevant box: $B_{(1)} = d^{1/2}$, $B_{(2)} = d^{1/4}$

Theorem (Katz 2006)

Bound(S_F) holds.

Theorem (LP 2006)

$$h_3(-d) \ll d^{\epsilon} N_{\mathcal{B}}(F) \ll d^{1/2-1/56}$$

Question: Can we get a nontrivial bound for $h_g(-d)$, $g \geq 5$?

- Relevant polynomial $F(x,z) = 4x^g - dz^2$
- Relevant modulus: $Q = d^{g/4-1/2+\delta}$, some $\delta > 0$
- Relevant box: $B_{(1)} = d^{1/2}$, $B_{(2)} = d^{g/4-1/2}$

Application to quadratic class group exponents

Quadratic field $\mathbb{Q}(\sqrt{-d})$
$E(-d)$ = exponent of $CL(-d)$: smallest positive integer r such that $[\mathfrak{a}]^r = I$ for all $[\mathfrak{a}] \in CL(-d)$

Conjecture

Given E, there are finitely many negative fundamental discriminants $-d$ such that $E(-d) = E$.

- $E = 2$: Euler
- $E = 3$: Boyd and Kisilevsky (1972), Weinberg (1973)
- GRH: $E(-d) \gg (\log d)/(\log\log d)$

Theorem (Heath-Brown 2008)

Let $E = 2^r$ or $E = 3 \cdot 2^r$ for any integer $r \geq 0$. Then there is an (ineffective) constant d_E such that $E(-d) \neq E$ for every fundamental discriminant $-d$ with $d > d_E$.

Class group exponent 5

Criterion for $E(-d) = 5$:
If $E(-d) = 5$ (and d is sufficiently large), then the equation

$$y^2 = 4x^5 - dz^2$$

has at least $d^{1/4}$ solutions with $x \ll d^{1/4+\epsilon}, z \ll d^{1/8+\epsilon}$.
Apply the split square sieve
Relevant polynomial: $F(x, z) = 4x^5 - dz^2$
Relevant modulus: $Q = d^{1/8+\delta}$, some $\delta > 0$
Relevant box: $B_{(1)} = d^{1/4+\epsilon}$, $B_{(2)} = d^{1/8+3\epsilon}$

Bound(S_F): (Katz 2006)

Theorem (Heath-Brown 2008)

There is an (ineffective) constant d_5 such that $E(-d) \neq 5$ for every fundamental discriminant $-d$ with $d > d_5$.