A variant of the large sieve inequality with explicit constants

Maciej Grześkowiak

Adam Mickiewicz University
Poznań, Poland

Number Theoretic Methods in Cryptology
Paris 2019

Outline

Outline

1. The large sieve inequality
2. The algorithmic number theory problem

Outline

1. The large sieve inequality
2. The algorithmic number theory problem
3. Application of the large sieve inequality

Outline

1. The large sieve inequality
2. The algorithmic number theory problem
3. Application of the large sieve inequality

The large sieve inequality

We define

$$S(x) = \sum_{n=M+1}^{M+N} c_n e(nx), \qquad e(\theta) = e^{2\pi i\theta},$$

where the c_n are arbitrary complex numbers.

The large sieve inequality

We define

$$S(x) = \sum_{n=M+1}^{M+N} c_n e(nx), \qquad e(\theta) = e^{2\pi i\theta},$$

where the c_n are arbitrary complex numbers.

The distance to nearest integer function

$$\|\theta\| = \min\{|\theta - n| : n \in \mathbb{Z}\}$$

The large sieve inequality

Let $x_1, \dots x_R$ be points which are well spaced modulo 1 in the sense that

$$\|x_r - x_s\| \geq \delta \tag{1}$$

for $s \neq r$, where $0 < \delta \leq \frac{1}{2}$.

The large sieve inequality

Let $x_1, \dots x_R$ be points which are well spaced modulo 1 in the sense that

$$\|x_r - x_s\| \geq \delta \tag{1}$$

for $s \neq r$, where $0 < \delta \leq \frac{1}{2}$.

The large sieve is an inequality of the form

$$\sum_{r=1}^{R} |S(x_r)|^2 \leq \Delta \sum_{n=M+1}^{M+N} |c_n|^2, \tag{2}$$

where $\Delta = \Delta(N, \delta)$.

The large sieve inequality

Let $x_1, \dots x_R$ be points which are well spaced modulo 1 in the sense that

$$\|x_r - x_s\| \geq \delta \tag{1}$$

for $s \neq r$, where $0 < \delta \leq \frac{1}{2}$.

The large sieve is an inequality of the form

$$\sum_{r=1}^{R} |S(x_r)|^2 \leq \Delta \sum_{n=M+1}^{M+N} |c_n|^2, \tag{2}$$

where $\Delta = \Delta(N, \delta)$.

[Gallagher] For example, we can take '$\Delta = \pi N + \delta^{-1}$

Application of the large sieve inequality

Let $x_r = \frac{a}{q}$ be points, where $(a, q) = 1$, $q \leq Q$, .
If $\frac{a}{q} \neq \frac{a'}{q'}$ then

Application of the large sieve inequality

Let $x_r = \frac{a}{q}$ be points, where $(a, q) = 1$, $q \leq Q$, .
If $\frac{a}{q} \neq \frac{a'}{q'}$ then

$$\left\| \frac{a}{q} - \frac{a'}{q'} \right\| = \left\| \frac{aq' - a'q}{qq'} \right\| \geq \frac{1}{qq'} \geq \frac{1}{Q^2}$$

We may take $\delta = Q^{-2}$, we obtain

Application of the large sieve inequality

Lemma

$$\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}|S(a/q)|^2\le (N+Q^2)\sum_{n=M+1}^{M+N}|c_n|^2,$$

where the summation is over primes q.

Application of the large sieve inequality

Let

$$\pi(x; a, q) = \sharp\{p \leq x : p \equiv a \pmod{q}, \quad (a, q) = 1\}$$

Application of the large sieve inequality

Let

$$\pi(x; a, q) = \sharp\{p \leq x : p \equiv a \pmod{q}, \quad (a, q) = 1\}$$

Then

$$\pi(x + y; a, q) - \pi(x; a, q) \leq \frac{2y}{\varphi(q) \log(y/q)} \left(1 + O\left(\frac{\log\log(3y/q)}{\log(2y/q)}\right)\right)$$

for $y > q$.

Application of the large sieve inequality

Let

$$T(\chi) = \sum_{n=M+1}^{M+N} c_n \chi(n)$$

where χ is a Dirichlet character $\pmod q$.

Application of the large sieve inequality

Let

$$T(\chi) = \sum_{n=M+1}^{M+N} c_n \chi(n)$$

where χ is a Dirichlet character $\pmod q$.

Gallagher show

$$\sum_{\chi \bmod q}^{*} |T(\chi)|^2 \leq \frac{\varphi(q)}{q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} |S(a/q)|^2$$

where $\sum^*$ denotes summation over primitive multiplicative characters χ $\pmod q$.

Application of the large sieve inequality

We obtain

$$\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi \bmod q}|T(\chi)|^2\le (N+Q^2)\sum_{n=M+1}^{M+N}|c_n|^2,$$

where the summation is over primes q and $\sum^*$ denotes summation over primitive multiplicative characters $\chi \pmod q$.

Generalization of the large sieve inequality

- Huxley generalized to algebraic number fields K, $[K : \mathbb{Q}] = k$.

Generalization of the large sieve inequality

- Huxley generalized to algebraic number fields K, $[K : \mathbb{Q}] = k$. He considered algebraic integers of $\alpha \in K$ such that

$$\alpha = n_1\omega_1 + \ldots + n_k\omega_k, \qquad M_i + 1 \leq n_i \leq M_i + N_i, \quad i = 1, \ldots k,$$

Generalization of the large sieve inequality

- Huxley generalized to algebraic number fields K, $[K : \mathbb{Q}] = k$. He considered algebraic integers of $\alpha \in K$ such that

$$\alpha = n_1\omega_1 + \ldots + n_k\omega_k, \qquad M_i + 1 \leq n_i \leq M_i + N_i, \quad i = 1, \ldots k,$$

- Schaal considered $\alpha \in K$ lying in the domains which not necessarily depend on special integer basis of K.

Generalization of the large sieve inequality

- Huxley generalized to algebraic number fields K, $[K : \mathbb{Q}] = k$. He considered algebraic integers of $\alpha \in K$ such that

$$\alpha = n_1\omega_1 + \ldots + n_k\omega_k, \qquad M_i + 1 \leq n_i \leq M_i + N_i, \quad i = 1, \ldots k,$$

- Schaal considered $\alpha \in K$ lying in the domains which not necessarily depend on special integer basis of K.
- Hinz proved a variant of the large sieve inequality to algebraic number K

Problem

Find two primes p and q such that

$$q \mid \sharp E(\mathbb{F}_p).$$

Problem

Find two primes p and q such that

$$q \mid \sharp E(\mathbb{F}_p).$$

Our assumptions

- p should be as close to q as possible

Problem

Find two primes p and q such that

$$q \mid \sharp E(\mathbb{F}_p).$$

Our assumptions

- p should be as close to q as possible
- works in a polynomial time with respect to p,

Problem

Find two primes p and q such that

$$q \mid \sharp E(\mathbb{F}_p).$$

Our assumptions

- p should be as close to q as possible
- works in a polynomial time with respect to p,
- give a proof without assumptions of any hypotheses, any heuristics,

Problem

Find two primes p and q such that

$$q \mid \sharp E(\mathbb{F}_p).$$

Our assumptions

- p should be as close to q as possible
- works in a polynomial time with respect to p,
- give a proof without assumptions of any hypotheses, any heuristics,
- compute the order of magnitude of p, q for which we can proof that the algorithm works

Application. Elliptic Curve Cryptography (ECC)

Theorem [Shparlinski, Sutherland 2014]

Given a real number $x > 3$.There is an Algorithm that outputs

$$p \in [x, 2x], \quad a, b \in \mathbb{F}_p, \quad N = \sharp E(\mathbb{F}_p),$$

where p is uniformly distributed over primes in $[x, 2x]$ and the pair (a, b) is then uniformly distributed over pairs in $\mathbb{F}_p \times \mathbb{F}_p$ for which $\sharp E(\mathbb{F}_p)$ is prime. Assuming the GRH, the expected running time of the Algorithm is

$$O((\log x)^5 (\log\log x)^3 \log\log\log x)$$

Application. Elliptic Curve Cryptography (ECC)

Theorem [Shparlinski, Sutherland 2017]

Assume the GRH. There is a deterministic algorithm that, given a prime p and an integer $m = o(p^{1/2}(\log p)^{-4})$, outputs an elliptic curve $E(\mathbb{F}_p)$ with $m \mid \sharp E(\mathbb{F}_p)$ in $O(mp^{1/2})$ time.

Application. Elliptic Curve Cryptography (ECC)

CM method:

Application. Elliptic Curve Cryptography (ECC)

CM method:

- select p,

Application. Elliptic Curve Cryptography (ECC)

CM method:

- select p,
- find $\Delta < 0$ and $s, t \in \mathbb{Z}$ such that $4p = t^2 - \Delta s^2$,

Application. Elliptic Curve Cryptography (ECC)

CM method:

- select p,
- find $\Delta < 0$ and $s, t \in \mathbb{Z}$ such that $4p = t^2 - \Delta s^2$,
- If $p + 1 \pm t$ is a prime, then construct E, or

Application. Elliptic Curve Cryptography (ECC)

CM method:

- select p,
- find $\Delta < 0$ and $s, t \in \mathbb{Z}$ such that $4p = t^2 - \Delta s^2$,
- If $p + 1 \pm t$ is a prime, then construct E, or
- If $p + 1 \pm t$ has a big prime factor q, then construct E,

CM-primes

CM-primes

DEFINITION:

CM-primes

DEFINITION:

Primes p and q are *CM-primes* with respect to $\Delta < 0$ if

CM-primes

DEFINITION:

Primes p and q are *CM-primes* with respect to $\Delta < 0$ if

there exist integers s and t such that

$$|t| \leq 2\sqrt{p}, \quad q|p+1-t, \quad 4p - t^2 = \Delta s^2.$$

CM-primes

DEFINITION:

Primes p and q are *CM-primes* with respect to $\Delta < 0$ if

there exist integers s and t such that

$$|t| \leq 2\sqrt{p}, \quad q|p+1-t, \quad 4p - t^2 = \Delta s^2.$$

Let p and q be CM-primes with respect to Δ.

CM-primes

DEFINITION:

Primes p and q are *CM-primes* with respect to $\Delta < 0$ if

there exist integers s and t such that

$$|t| \leq 2\sqrt{p}, \quad q|p+1-t, \quad 4p - t^2 = \Delta s^2.$$

Let p and q be CM-primes with respect to Δ.

There exist $E(\mathbb{F}_p)$ such that $q \mid \sharp E(\mathbb{F}_p) = p + 1 - t$

CM-primes

DEFINITION:

Primes p and q are *CM-primes* with respect to $\Delta < 0$ if

there exist integers s and t such that

$$|t| \leq 2\sqrt{p}, \quad q|p+1-t, \quad 4p - t^2 = \Delta s^2.$$

Let p and q be CM-primes with respect to Δ.

There exist $E(\mathbb{F}_p)$ such that $q \mid \sharp E(\mathbb{F}_p) = p + 1 - t$

To construct E we use CM method, $\quad O(|\Delta|^{1+\epsilon})$,

CM-primes

DEFINITION:

Primes p and q are *CM-primes* with respect to $\Delta < 0$ if

there exist integers s and t such that

$$|t| \leq 2\sqrt{p}, \quad q|p+1-t, \quad 4p - t^2 = \Delta s^2.$$

Let p and q be CM-primes with respect to Δ.

There exist $E(\mathbb{F}_p)$ such that $q \mid \sharp E(\mathbb{F}_p) = p + 1 - t$

To construct E we use CM method, $\quad O(|\Delta|^{1+\epsilon}), \quad \Delta \leq 10^{12}$

CM-primes

- $K = \mathbb{Q}(\sqrt{\Delta}), \quad \Delta \equiv 1 \pmod 4, \quad \omega = \frac{1+\sqrt{\Delta}}{2}$

CM-primes

- $K = \mathbb{Q}(\sqrt{\Delta}), \quad \Delta \equiv 1 \pmod 4, \quad \omega = \frac{1+\sqrt{\Delta}}{2}$
- $\mathcal{O}_K = \{a + b\omega : a, b \in \mathbb{Z}\}$,

CM-primes

- $K = \mathbb{Q}(\sqrt{\Delta}), \quad \Delta \equiv 1 \pmod 4, \quad \omega = \frac{1+\sqrt{\Delta}}{2}$
- $\mathcal{O}_K = \{a + b\omega : a, b \in \mathbb{Z}\}$,

Input: $n, m \in \mathbb{N}$, $(m, n) = 1$, $x \in \mathbb{R}$,

CM-primes

- $K = \mathbb{Q}(\sqrt{\Delta}), \quad \Delta \equiv 1 \pmod 4, \quad \omega = \frac{1+\sqrt{\Delta}}{2}$
- $\mathcal{O}_K = \{a + b\omega : a, b \in \mathbb{Z}\}$,

Input: $n, m \in \mathbb{N}$, $(m, n) = 1$, $x \in \mathbb{R}$,
$\gamma = f + g\omega \in \mathcal{O}_K$, $|f|, |g| \leq n$, $N_{K/\mathbb{Q}}(\gamma) \equiv m \pmod n$

CM-primes

- $K = \mathbb{Q}(\sqrt{\Delta}), \quad \Delta \equiv 1 \pmod 4, \quad \omega = \frac{1+\sqrt{\Delta}}{2}$
- $\mathcal{O}_K = \{a + b\omega : a, b \in \mathbb{Z}\}$,

Input: $n, m \in \mathbb{N}$, $(m, n) = 1$, $x \in \mathbb{R}$,
$\gamma = f + g\omega \in \mathcal{O}_K$, $|f|, |g| \leq n$, $N_{K/\mathbb{Q}}(\gamma) \equiv m \pmod n$

Procedure FindPrimeQ (MG)

CM-primes

- $K = \mathbb{Q}(\sqrt{\Delta}), \quad \Delta \equiv 1 \pmod 4, \quad \omega = \frac{1+\sqrt{\Delta}}{2}$
- $\mathcal{O}_K = \{a + b\omega : a, b \in \mathbb{Z}\}$,

Input: $n, m \in \mathbb{N}$, $(m, n) = 1$, $x \in \mathbb{R}$,
$\gamma = f + g\omega \in \mathcal{O}_K$, $|f|, |g| \leq n$, $N_{K/\mathbb{Q}}(\gamma) \equiv m \pmod n$

Procedure FindPrimeQ (MG)

1. Find

$$|u| \leq (\frac{\sqrt{1-\Delta}}{\sqrt{-4\Delta}}(2x)^{1/2} - f)n^{-1}, \quad |v| \leq (\frac{1}{\sqrt{-\Delta}}(2x)^{1/2} - g)n^{-1}$$

CM-primes

- $K = \mathbb{Q}(\sqrt{\Delta}), \quad \Delta \equiv 1 \pmod 4, \quad \omega = \frac{1+\sqrt{\Delta}}{2}$
- $\mathcal{O}_K = \{a + b\omega : a, b \in \mathbb{Z}\}$,

Input: $n, m \in \mathbb{N}$, $(m, n) = 1$, $x \in \mathbb{R}$,
$\gamma = f + g\omega \in \mathcal{O}_K$, $|f|, |g| \leq n$, $N_{K/\mathbb{Q}}(\gamma) \equiv m \pmod n$

Procedure FindPrimeQ (MG)

1. Find

$$|u| \leq (\frac{\sqrt{1-\Delta}}{\sqrt{-4\Delta}}(2x)^{1/2} - f)n^{-1}, \quad |v| \leq (\frac{1}{\sqrt{-\Delta}}(2x)^{1/2} - g)n^{-1}$$

2. Compute $\alpha = nu + f + (nv + g)\omega$

CM-primes

- $K = \mathbb{Q}(\sqrt{\Delta}), \quad \Delta \equiv 1 \pmod 4, \quad \omega = \frac{1+\sqrt{\Delta}}{2}$
- $\mathcal{O}_K = \{a + b\omega : a, b \in \mathbb{Z}\}$,

Input: $n, m \in \mathbb{N}$, $(m, n) = 1$, $x \in \mathbb{R}$,
$\gamma = f + g\omega \in \mathcal{O}_K$, $|f|, |g| \leq n$, $N_{K/\mathbb{Q}}(\gamma) \equiv m \pmod n$

Procedure FindPrimeQ (MG)

1. Find

$$|u| \leq (\frac{\sqrt{1-\Delta}}{\sqrt{-4\Delta}}(2x)^{1/2} - f)n^{-1}, \quad |v| \leq (\frac{1}{\sqrt{-\Delta}}(2x)^{1/2} - g)n^{-1}$$

2. Compute $\alpha = nu + f + (nv + g)\omega$
3. If $q = N_{K/\mathbb{Q}}(\alpha)$ is a prime,

CM-primes

- $K = \mathbb{Q}(\sqrt{\Delta}), \quad \Delta \equiv 1 \pmod 4, \quad \omega = \frac{1+\sqrt{\Delta}}{2}$
- $\mathcal{O}_K = \{a + b\omega : a, b \in \mathbb{Z}\}$,

Input: $n, m \in \mathbb{N}$, $(m, n) = 1$, $x \in \mathbb{R}$,
$\gamma = f + g\omega \in \mathcal{O}_K$, $|f|, |g| \leq n$, $N_{K/\mathbb{Q}}(\gamma) \equiv m \pmod n$

Procedure FindPrimeQ (MG)

1. Find

$$|u| \leq (\frac{\sqrt{1-\Delta}}{\sqrt{-4\Delta}}(2x)^{1/2} - f)n^{-1}, \quad |v| \leq (\frac{1}{\sqrt{-\Delta}}(2x)^{1/2} - g)n^{-1}$$

2. Compute $\alpha = nu + f + (nv + g)\omega$
3. If $q = N_{K/\mathbb{Q}}(\alpha)$ is a prime, then RETURN $\alpha = a + b\omega$ and q

CM-primes

Input: $K = \mathbb{Q}(\sqrt{\Delta})$, $\alpha = a + b\omega \in \mathcal{O}_K$, $q = N_{K/\mathbb{Q}}(\alpha) \equiv m \pmod{n}$, $\Delta \equiv 1 \pmod 4$, $0 < \varepsilon < 2/5$

CM-primes

Input: $K = \mathbb{Q}(\sqrt{\Delta})$, $\alpha = a + b\omega \in \mathcal{O}_K$, $q = N_{K/\mathbb{Q}}(\alpha) \equiv m \pmod{n}$, $\Delta \equiv 1 \pmod 4$, $0 < \varepsilon < 2/5$

Procedure FindPrimeP (MG)

CM-primes

Input: $K = \mathbb{Q}(\sqrt{\Delta})$, $\alpha = a + b\omega \in \mathcal{O}_K$, $q = N_{K/\mathbb{Q}}(\alpha) \equiv m \pmod{n}$, $\Delta \equiv 1 \pmod 4$, $0 < \varepsilon < 2/5$

Procedure FindPrimeP (MG)

1. Find

$$|s| \leq \frac{\sqrt{1-\Delta}}{\sqrt{-4\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}, \quad |t| \leq \frac{1}{\sqrt{-\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}.$$

CM-primes

Input: $K = \mathbb{Q}(\sqrt{\Delta})$, $\alpha = a + b\omega \in \mathcal{O}_K$, $q = N_{K/\mathbb{Q}}(\alpha) \equiv m \pmod{n}$, $\Delta \equiv 1 \pmod 4$, $0 < \varepsilon < 2/5$

Procedure FindPrimeP (MG)

1. Find

$$|s| \leq \frac{\sqrt{1-\Delta}}{\sqrt{-4\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}, \quad |t| \leq \frac{1}{\sqrt{-\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}.$$

2. Compute $\beta = as - \frac{1-\Delta}{4}bt + 1 + (bs + (a+b)t)\omega$

CM-primes

Input: $K = \mathbb{Q}(\sqrt{\Delta})$, $\alpha = a + b\omega \in \mathcal{O}_K$, $q = N_{K/\mathbb{Q}}(\alpha) \equiv m \pmod{n}$, $\Delta \equiv 1 \pmod 4$, $0 < \varepsilon < 2/5$

Procedure FindPrimeP (MG)

1. Find

$$|s| \leq \frac{\sqrt{1-\Delta}}{\sqrt{-4\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}, \quad |t| \leq \frac{1}{\sqrt{-\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}.$$

2. Compute $\beta = as - \frac{1-\Delta}{4}bt + 1 + (bs + (a+b)t)\omega$
3. Compute $p = N_{K/\mathbb{Q}}(\beta)$

CM-primes

Input: $K = \mathbb{Q}(\sqrt{\Delta})$, $\alpha = a + b\omega \in \mathcal{O}_K$, $q = N_{K/\mathbb{Q}}(\alpha) \equiv m \pmod{n}$, $\Delta \equiv 1 \pmod 4$, $0 < \varepsilon < 2/5$

Procedure FindPrimeP (MG)

1. Find

$$|s| \leq \frac{\sqrt{1-\Delta}}{\sqrt{-4\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}, \quad |t| \leq \frac{1}{\sqrt{-\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}.$$

2. Compute $\beta = as - \frac{1-\Delta}{4}bt + 1 + (bs + (a+b)t)\omega$
3. Compute $p = N_{K/\mathbb{Q}}(\beta)$
4. If $p < x$ or $p > (2x)^{5/(2-5\varepsilon)}$ is a prime, then

CM-primes

Input: $K = \mathbb{Q}(\sqrt{\Delta})$, $\alpha = a + b\omega \in \mathcal{O}_K$, $q = N_{K/\mathbb{Q}}(\alpha) \equiv m \pmod{n}$, $\Delta \equiv 1 \pmod 4$, $0 < \varepsilon < 2/5$

Procedure FindPrimeP (MG)

1. Find

$$|s| \leq \frac{\sqrt{1-\Delta}}{\sqrt{-4\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}, \quad |t| \leq \frac{1}{\sqrt{-\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}.$$

2. Compute $\beta = as - \frac{1-\Delta}{4}bt + 1 + (bs + (a+b)t)\omega$
3. Compute $p = N_{K/\mathbb{Q}}(\beta)$
4. If $p < x$ or $p > (2x)^{5/(2-5\varepsilon)}$ is a prime, then
5. RETURN $\beta = c + d\omega$, p.

CM-primes

Input: $K = \mathbb{Q}(\sqrt{\Delta})$, $\alpha = a + b\omega \in \mathcal{O}_K$, $q = N_{K/\mathbb{Q}}(\alpha) \equiv m \pmod{n}$, $\Delta \equiv 1 \pmod 4$, $0 < \varepsilon < 2/5$

Procedure FindPrimeP (MG)

1. Find

$$|s| \leq \frac{\sqrt{1-\Delta}}{\sqrt{-4\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}, \quad |t| \leq \frac{1}{\sqrt{-\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}.$$

2. Compute $\beta = as - \frac{1-\Delta}{4}bt + 1 + (bs + (a+b)t)\omega$
3. Compute $p = N_{K/\mathbb{Q}}(\beta)$
4. If $p < x$ or $p > (2x)^{5/(2-5\varepsilon)}$ is a prime, then
5. RETURN $\beta = c + d\omega$, p.

$\beta \equiv 1 \pmod{\alpha}$,

CM-primes

Input: $K = \mathbb{Q}(\sqrt{\Delta})$, $\alpha = a + b\omega \in \mathcal{O}_K$, $q = N_{K/\mathbb{Q}}(\alpha) \equiv m \pmod{n}$, $\Delta \equiv 1 \pmod 4$, $0 < \varepsilon < 2/5$

Procedure FindPrimeP (MG)

1. Find

$$|s| \leq \frac{\sqrt{1-\Delta}}{\sqrt{-4\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}, \quad |t| \leq \frac{1}{\sqrt{-\Delta}}(2x)^{(3+5\varepsilon)/(4-10\varepsilon)}.$$

2. Compute $\beta = as - \frac{1-\Delta}{4}bt + 1 + (bs + (a+b)t)\omega$
3. Compute $p = N_{K/\mathbb{Q}}(\beta)$
4. If $p < x$ or $p > (2x)^{5/(2-5\varepsilon)}$ is a prime, then
5. RETURN $\beta = c + d\omega$, p.

$\beta \equiv 1 \pmod{\alpha}$, $N_{K/\mathbb{Q}}(\alpha) \mid N_{K/\mathbb{Q}}(\beta - 1) = N_{K/\mathbb{Q}}(\beta) + 1 - Tr(\beta)$

CM-primes

Theorem [M.G.2015]

- There exists $x_0 > 0$ such that for every $x \geq x_0$ and $\lambda \in \mathbb{R}$, $\lambda \geq 1$,

CM-primes

Theorem [M.G.2015]

- There exists $x_0 > 0$ such that for every $x \geq x_0$ and $\lambda \in \mathbb{R}$, $\lambda \geq 1$,
- procedure FindPrimeQ finds

$$\alpha \in \mathcal{O}_K, \quad q = N_{K/\mathbb{Q}}(\alpha) \equiv m \pmod{n}, \quad x \leq N_{K/\mathbb{Q}}(\alpha) \leq 2x$$

CM-primes

Theorem [M.G.2015]

- There exists $x_0 > 0$ such that for every $x \geq x_0$ and $\lambda \in \mathbb{R}$, $\lambda \geq 1$,
- procedure FindPrimeQ finds

$$\alpha \in \mathcal{O}_K, \quad q = N_{K/\mathbb{Q}}(\alpha) \equiv m \pmod{n}, \quad x \leq N_{K/\mathbb{Q}}(\alpha) \leq 2x$$

- with probability greater than or equal to $1 - e^{-\lambda}$

CM-primes

Theorem [M.G.2015]

- There exists $x_0 > 0$ such that for every $x \geq x_0$ and $\lambda \in \mathbb{R}$, $\lambda \geq 1$,
- procedure FindPrimeQ finds

$$\alpha \in \mathcal{O}_K, \quad q = N_{K/\mathbb{Q}}(\alpha) \equiv m \pmod{n}, \quad x \leq N_{K/\mathbb{Q}}(\alpha) \leq 2x$$

- with probability greater than or equal to $1 - e^{-\lambda}$
- after repeating $[c_1 \lambda (\log x)]$ steps,

CM-primes

Theorem [M.G.2015]

- There exists $x_0 > 0$ such that for every $x \geq x_0$ and $\lambda \in \mathbb{R}$, $\lambda \geq 1$,
- procedure FindPrimeQ finds

$$\alpha \in \mathcal{O}_K, \quad q = N_{K/\mathbb{Q}}(\alpha) \equiv m \pmod{n}, \quad x \leq N_{K/\mathbb{Q}}(\alpha) \leq 2x$$

- with probability greater than or equal to $1 - e^{-\lambda}$
- after repeating $[c_1 \lambda (\log x)]$ steps,
- where $c_1 = \frac{4\sqrt{1-\Delta} h^*_{\mathfrak{f}}(K)}{-\Delta n^2}$, $\mathfrak{f} = n\mathcal{O}_K$.

CM-primes

Theorem [M.G.2015]

- There exists $x_0 > 0$ such that for every $x \geq x_0$ and $\lambda \in \mathbb{R}$, $\lambda \geq 1$,
- procedure FindPrimeQ finds

$$\alpha \in \mathcal{O}_K, \quad q = N_{K/\mathbb{Q}}(\alpha) \equiv m \pmod{n}, \quad x \leq N_{K/\mathbb{Q}}(\alpha) \leq 2x$$

- with probability greater than or equal to $1 - e^{-\lambda}$
- after repeating $[c_1 \lambda (\log x)]$ steps,
- where $c_1 = \frac{4\sqrt{1-\Delta} h^*_{\mathfrak{f}}(K)}{-\Delta n^2}$, $\mathfrak{f} = n\mathcal{O}_K$.

CM-primes

Theorem [MG 2015]

- Let $\alpha \in \mathcal{O}_K$, $\quad x \leq q = N_{K/\mathbb{Q}}(\alpha) \leq 2x$.

CM-primes

Theorem [MG 2015]

- Let $\alpha \in \mathcal{O}_K$, $\quad x \leq q = N_{K/\mathbb{Q}}(\alpha) \leq 2x$.
- there exists $x_0 > 0$ such that for every $x \geq x_0$, and for $\lambda \in \mathbb{R}$, $\lambda \geq 1$, and for any $A > 2$

CM-primes

Theorem [MG 2015]

- Let $\alpha \in \mathcal{O}_K, \quad x \leq q = N_{K/\mathbb{Q}}(\alpha) \leq 2x.$
- there exists $x_0 > 0$ such that for every $x \geq x_0$, and for $\lambda \in \mathbb{R}$, $\lambda \geq 1$, and for any $A > 2$
- procedure FindPrimeP finds
  $\beta = c + d\omega, \quad p = N_{K/\mathbb{Q}}(\beta), x \leq N_{K/\mathbb{Q}}(\beta) \leq (2x)^{5/(2-5\varepsilon)},$

CM-primes

Theorem [MG 2015]

- Let $\alpha \in \mathcal{O}_K, \quad x \leq q = N_{K/\mathbb{Q}}(\alpha) \leq 2x.$
- there exists $x_0 > 0$ such that for every $x \geq x_0$, and for $\lambda \in \mathbb{R}$, $\lambda \geq 1$, and for any $A > 2$
- procedure FindPrimeP finds
  $\beta = c + d\omega, \quad p = N_{K/\mathbb{Q}}(\beta), x \leq N_{K/\mathbb{Q}}(\beta) \leq (2x)^{5/(2-5\varepsilon)},$
- with probability greater than or equal to $1 - e^{-\lambda}$ after repeating $[c_2\lambda(\log 2x)]$ steps of the procedure,

CM-primes

Theorem [MG 2015]

- Let $\alpha \in \mathcal{O}_K, \quad x \leq q = N_{K/\mathbb{Q}}(\alpha) \leq 2x.$
- there exists $x_0 > 0$ such that for every $x \geq x_0$, and for $\lambda \in \mathbb{R}$, $\lambda \geq 1$, and for any $A > 2$
- procedure FindPrimeP finds
  $\beta = c + d\omega, \quad p = N_{K/\mathbb{Q}}(\beta), \; x \leq N_{K/\mathbb{Q}}(\beta) \leq (2x)^{5/(2-5\varepsilon)},$
- with probability greater than or equal to $1 - e^{-\lambda}$ after repeating $[c_2\lambda(\log 2x)]$ steps of the procedure,
- for almost all α with the possible exception of at most $O(x(\log x)^{-A})$ values of α, where $c_2 = \frac{40h(K)\sqrt{1-\Delta}}{-(2-5\varepsilon)w(K)\Delta}$

Notation

- K - any totally imaginary algebraic number field of degree $[K : \mathbb{Q}] = 2r_2$,

Notation

- K - any totally imaginary algebraic number field of degree $[K : \mathbb{Q}] = 2r_2$,

- $\mathfrak{f}$ - a given non-zero integral ideal of the ring of $\mathcal{O}_K$,

Notation

- K - any totally imaginary algebraic number field of degree $[K : \mathbb{Q}] = 2r_2$,
- $\mathfrak{f}$ - a given non-zero integral ideal of the ring of $\mathcal{O}_K$,
- $H \pmod{\mathfrak{f}}$ - any ideal class mod $\mathfrak{f}$ in the "narrow" sense,

Notation

- K - any totally imaginary algebraic number field of degree $[K : \mathbb{Q}] = 2r_2$,
- $\mathfrak{f}$ - a given non-zero integral ideal of the ring of $\mathcal{O}_K$,
- $H \pmod{\mathfrak{f}}$ - any ideal class mod $\mathfrak{f}$ in the "narrow" sense,
- $h^*_{\mathfrak{f}}(K)$ - the number of elements of H,

Notation

- K - any totally imaginary algebraic number field of degree $[K : \mathbb{Q}] = 2r_2$,
- $\mathfrak{f}$ - a given non-zero integral ideal of the ring of $\mathcal{O}_K$,
- $H \pmod{\mathfrak{f}}$ - any ideal class mod $\mathfrak{f}$ in the "narrow" sense,
- $h^*_{\mathfrak{f}}(K)$ - the number of elements of H,
- Let $s = \sigma + it$

$$\zeta(s, \chi) = \sum_{\mathfrak{a} \in \mathcal{O}_K} \frac{\chi(\mathfrak{a})}{(N\mathfrak{a})^s}, \qquad \sigma > 1,$$

where $\mathfrak{a}$ runs through integral ideals of $\mathcal{O}_K$

Notation

- χ_0 denote the principal character modulo $\mathfrak{f}$

Notation

- χ_0 denote the principal character modulo $\mathfrak{f}$
- Let

$$E_0 = E_0(\chi) = \begin{cases} 1 & \text{for} \quad \chi = \chi_0 \\ 0 & \text{for} \quad \chi \neq \chi_0 \end{cases}$$

Notation

- χ_0 denote the principal character modulo $\mathfrak{f}$
- Let

$$E_0 = E_0(\chi) = \begin{cases} 1 & \text{for} \quad \chi = \chi_0 \\ 0 & \text{for} \quad \chi \neq \chi_0 \end{cases}$$

- Fix $X \mod \mathfrak{f} \in H$.

Notation

- χ_0 denote the principal character modulo $\mathfrak{f}$
- Let

$$E_0 = E_0(\chi) = \begin{cases} 1 & \text{for} \quad \chi = \chi_0 \\ 0 & \text{for} \quad \chi \neq \chi_0 \end{cases}$$

- Fix $X \mod \mathfrak{f} \in H$.

$$\Psi(x, X) = \sum_{\substack{x \leq N\mathfrak{p}^m \leq 2x \\ \mathfrak{p}^m \in X}} \log N\mathfrak{p},$$

where $\mathfrak{p}$ runs through prime ideals of $\mathcal{O}_K$

Theorem [M. G. 2017]

If $|\Delta| \geq 9$ and there is no zero in the region

$$\sigma \geq 1 - 0.0795 \left(\log |\Delta| + 0.7761 \log \left((|t|+1)^{2r_2} (N\mathfrak{f})^{1-E_0(\chi)} \right) \right)^{-1},$$

then

Theorem [M. G. 2017]

If $|\Delta| \geq 9$ and there is no zero in the region

$$\sigma \geq 1 - 0.0795 \left(\log |\Delta| + 0.7761 \log \left((|t|+1)^{2r_2} (N\mathfrak{f})^{1-E_0(\chi)} \right) \right)^{-1},$$

then

$$\Psi(x, X) \geq \frac{x}{2h_{\mathfrak{f}}^*(K)},$$

Theorem [M. G. 2017]

If $|\Delta| \geq 9$ and there is no zero in the region

$$\sigma \geq 1 - 0.0795 \left(\log |\Delta| + 0.7761 \log \left((|t|+1)^{2r_2} (N\mathfrak{f})^{1-E_0(\chi)} \right) \right)^{-1},$$

then

$$\Psi(x, X) \geq \frac{x}{2h_{\mathfrak{f}}^*(K)},$$

for $\log x \geq$

$$\left(23.441\sqrt{r_2} \left(1 + (2\log(17.252C\sqrt{r_2}))^{\frac{1}{2}} + \frac{2}{3}\log(17.252C\sqrt{r_2}) \right) \right)^2,$$

Theorem [M. G. 2017]

If $|\Delta| \geq 9$ and there is no zero in the region

$$\sigma \geq 1 - 0.0795 \left(\log |\Delta| + 0.7761 \log \left((|t|+1)^{2r_2} (N\mathfrak{f})^{1-E_0(\chi)} \right) \right)^{-1},$$

then

$$\Psi(x, X) \geq \frac{x}{2h_{\mathfrak{f}}^*(K)},$$

for $\log x \geq$

$$\left(23.441\sqrt{r_2} \left(1 + (2\log(17.252C\sqrt{r_2}))^{\frac{1}{2}} + \frac{2}{3}\log(17.252C\sqrt{r_2}) \right) \right)^2,$$

where

$$C = (3056|\Delta|^{\frac{1.933}{r_2}} + 15382.485|\Delta|^{\frac{1.289}{r_2}} (N\mathfrak{f})^{\frac{1}{r_2}} h_{\mathfrak{f}}^*(K)) r_2^2 \log(|\Delta| N\mathfrak{f}).$$

Notation

- Let $D < 0$ be a square-free integer,
- Let $K = \mathbb{Q}(\sqrt{D})$ with $\mathcal{O}_K = \{a + b\omega : a, b \in \mathbb{Z}\}$, where

$$\omega = \begin{cases} \frac{1+\sqrt{D}}{2} & \text{if} \quad D \equiv 1 \pmod 4 \\ \sqrt{D} & \text{if} \quad D \equiv 2, 3 \pmod 4 \end{cases}$$

Let $x > 1$, we define

$$\mathfrak{R} = \{\beta \in \mathcal{O}_K : \quad |\beta| < \sqrt{x}\}.$$

Theorem [M. G. 2019]

Fix $Q > 1$,

$$\sum_{\substack{N\mathfrak{q}\leq Q\\(\mathfrak{q},\mathfrak{a})=1}} \sideset{}{'}\sum_{\sigma \bmod \mathfrak{q}} \left| \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\sigma(\alpha)\right|^2 \leq f(x,\mathfrak{a},Q) \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} |c(\alpha)|^2,$$

Theorem [M. G. 2019]

Fix $Q > 1$,

$$\sum_{\substack{N\mathfrak{q}\leq Q\\(\mathfrak{q},\mathfrak{a})=1}} \sum_{\sigma \bmod \mathfrak{q}}{}' \left| \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\sigma(\alpha)\right|^2 \leq f(x,\mathfrak{a},Q) \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} |c(\alpha)|^2,$$

where $f(x,\mathfrak{a},Q) = \left(\frac{\sqrt{8}}{\sqrt[4]{3}}\left(\frac{x}{N\mathfrak{a}}\right)^{\frac{1}{4}} + c_0|D|^{\frac{1}{4}}Q^{\frac{1}{2}}\right)^4$,

$$c_0 = \begin{cases} \left(1-\frac{1}{\sqrt{3}}\right)^{-\frac{1}{2}} & \text{if} \quad D\equiv 1 \pmod 4,\\ \left(\frac{1}{2}-\frac{1}{2\sqrt{3}}\right)^{-\frac{1}{2}} & \text{if} \quad D\equiv 2,3 \pmod 4,\end{cases}$$

and $\sum'$ denotes summation over primitive additive characters $\pmod{\mathfrak{q}}$, and the $c(\alpha)$ are any complex number.

Theorem [M. G. 2019]

Fix $Q > 1$. We have

$$\sum_{N\mathfrak{q}\leq Q} \frac{N\mathfrak{q}}{\Phi(\mathfrak{q})} \sideset{}{^*}\sum_{\chi \bmod \mathfrak{q}} \left| \sum_{\substack{\alpha\in\mathfrak{R} \\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\chi(\alpha) \right|^2 \leq f(x,\mathfrak{a},Q) \sum_{\substack{\alpha\in\mathfrak{R} \\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} |c(\alpha)|^2,$$

Theorem [M. G. 2019]

Fix $Q > 1$. We have

$$\sum_{N\mathfrak{q}\le Q} \frac{N\mathfrak{q}}{\Phi(\mathfrak{q})} \sideset{}{^*}\sum_{\chi \bmod \mathfrak{q}} \left| \sum_{\substack{\alpha\in\mathfrak{R} \\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\chi(\alpha) \right|^2 \le f(x,\mathfrak{a},Q) \sum_{\substack{\alpha\in\mathfrak{R} \\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} |c(\alpha)|^2,$$

where $f(x,\mathfrak{a},Q) = \left(\frac{\sqrt{8}}{\sqrt[4]{3}} \left(\frac{x}{N\mathfrak{a}}\right)^{\frac{1}{4}} + c_0 |D|^{\frac{1}{4}} Q^{\frac{1}{2}} \right)^4$,

$$c_0 = \begin{cases} \left(1 - \frac{1}{\sqrt{3}}\right)^{-\frac{1}{2}} & \text{if} \quad D \equiv 1 \pmod 4, \\ \left(\frac{1}{2} - \frac{1}{2\sqrt{3}}\right)^{-\frac{1}{2}} & \text{if} \quad D \equiv 2,3 \pmod 4, \end{cases}$$

and $\sum^*$ denotes summation over primitive multiplicative characters (mod $\mathfrak{q}$), and the $c(\alpha)$ are any complex numbers.

Thank you