An Almost-Prime Sieve in Algebraic Number Field

Kong-ching Lee

師大學報 第二十四期

Let K be a real quadratic number field with the discriminant d, z a positive number and $P = P(z) = \prod_{Np \leq z} p$, where N denotes the norm. For the integers ξ and α in K we define $\sigma_\alpha(\xi)$ to be the greatest common divisor of $\xi - \alpha$ and P(z). Let $\mathcal{A}_k$ denote the set of integers ξ in the rectangular

$$0 < \xi \leq x \ , \ 0 < \xi' \leq x'$$

such that

$$V(\sigma_\alpha(\xi)) < K \ ,$$

where $V(\mathfrak{n})$ is the number of distinct prime factors of ideal $\mathfrak{n}$, and ξ' the conjugate of ξ.

In this paper we will estimate the number of elements of $\mathcal{A}_k$. We need the following lemmata.

Lemma 1 : Let $\mu_k(\mathfrak{n}) = \mu(\mathfrak{n}) \ (-1)^{k-1} \binom{V(\mathfrak{n})-1}{k-1}$

then $\mu_k(\mathfrak{n}) = \sum\limits_{i=0}^{k-1} \mu(\mathfrak{n}) \ (-1)^i \binom{V(\mathfrak{n})}{i}$

Proof : Since

$$\sum_{i=0}^{k-1} (-1)^i \binom{V(\mathfrak{n})}{i} = \sum_{i=0}^{k-1} (-1)^i \left\{ \binom{V(\mathfrak{n})-1}{i-1} + \binom{V(\mathfrak{n})-1}{i} \right\}$$

$$= \sum_{i=1}^{k-1} (-1)^i \binom{V(\mathfrak{n})-1}{i-1} + \sum_{i=1}^{k} (-1)^{i-1} \binom{V(\mathfrak{n})-1}{i=1}$$

$$= (-1)^{k-1} \binom{V(\mathfrak{n})-1}{k-1}$$

Hence we have

$$\mu_k(\mathfrak{n}) = \sum_{i=0}^{k-1} \mu(\mathfrak{n}) \ (-1)^i \binom{V(\mathfrak{n})}{i}$$

The function $\mu_k(\mathfrak{n})$ has the following property:

Lemma 2 : If $V(\mathfrak{q})<k$, $\sum_{\mathfrak{n}|\mathfrak{q}}\mu_k(\mathfrak{n})=1$; if $V(\mathfrak{q})\geqslant k$, $\sum_{\mathfrak{n}|\mathfrak{q}}\mu_k(\mathfrak{n})=0$

Proof : If $V(\mathfrak{q})<k$, then $V(\mathfrak{n})\leqslant k-1$ for each $\mathfrak{n}|\mathfrak{q}$, hence

$$\mu_k(\mathfrak{n})=\sum_{i=0}^{k-1}\mu(\mathfrak{n})\,(-1)^i\binom{V(\mathfrak{n})}{i}$$

$$=\mu(\mathfrak{n})\sum_{i=0}^{V(\mathfrak{n})}(-1)^i\binom{V(\mathfrak{n})}{i}$$

$$=\begin{cases}1, & \text{if } \mathfrak{n}=(1)\\ 0, & \text{if } \mathfrak{n}\neq(1)\end{cases}$$

Therefore,

$$\sum_{\mathfrak{n}|\mathfrak{q}}\mu_k(\mathfrak{n})=1$$

If $v(\mathfrak{q})\geqslant k$, we have

$$\sum_{\mathfrak{n}|\mathfrak{q}}\mu_k(\mathfrak{n})=\sum_{\mathfrak{n}|\mathfrak{q}}\sum_{i=0}^{k-1}\mu(\mathfrak{n})\,(-1)^i\binom{V(\mathfrak{n})}{i}$$

$$=\sum_{m=0}^{V(\mathfrak{q})}\binom{V(\mathfrak{q})}{m}\sum_{i=0}^{k-1}(-1)^{m+i}\binom{m}{i}$$

$$=\sum_{i=0}^{k-1}(-1)^i\sum_{m=i}^{V(\mathfrak{q})}(-1)^m\binom{V(\mathfrak{q})}{m}\binom{m}{i}$$

$$=\sum_{i=0}^{k-1}(-1)^i\sum_{m=i}^{V(\mathfrak{q})}(-1)^m\binom{V(\mathfrak{q})}{i}\binom{V(\mathfrak{q})-i}{m-i}$$

$$=\sum_{i=0}^{k-1}(-1)^i\binom{V(\mathfrak{q})}{i}\sum_{m=i}^{V(\mathfrak{q})}(-1)^m\binom{V(\mathfrak{q})-1}{m-1}$$

$=0$, for the inner sum is equal to 0.

Now, we define the function $\varphi_k(\mathfrak{q})$ to be the number of ξ mod $\mathfrak{q}$ such that $V(\xi,\mathfrak{q})<k$, then we have

Lemma 3 : For $\mathfrak{q}$ square free, $\sum_{\mathfrak{n}|\mathfrak{q}}\frac{\mu_k(\mathfrak{n})}{N\mathfrak{n}}=\frac{\varphi_k(\mathfrak{q})}{N\mathfrak{q}}$

Proof : $\varphi_k(\eta) = \sum\limits_{\substack{\xi \bmod \eta \\ V(\xi,\eta)<k}} 1 = \sum\limits_{\xi \bmod \eta} \sum\limits_{\substack{\mathfrak{n}|\xi \\ \mathfrak{n}|\eta}} \mu_k(\mathfrak{n})$

$$= \sum_{\mathfrak{n}|\eta} \mu_k(\mathfrak{n}) \sum_{\substack{\xi \bmod \eta \\ \xi \equiv 0 \pmod{\mathfrak{n}}}}$$

$$= \sum_{\mathfrak{n}|\eta} \mu_k(\mathfrak{n}) \frac{N\eta}{N\mathfrak{n}}$$

Hence

$$\sum_{\mathfrak{n}|\eta} \frac{\mu_k(\mathfrak{n})}{N\mathfrak{n}} = \frac{\varphi_k(\eta)}{N\eta}$$

Lemma 4: Let $\theta_k(\eta, m) = \sum\limits_{\substack{\mathfrak{n}|\eta \\ V(\mathfrak{n}) \leq m}} \mu_k(\mathfrak{n})$, then we have the following:

(1) If $k > V(\eta)$ or $k > m$, then $\theta_k(\eta, m) = 1$

(2) If $k \leqslant V(\eta) \leqslant m$, then $\theta_k(\eta, m) = 0$

(3) If $k \leqslant m < V(\eta)$, then $\theta_k(\eta, m) \geqslant 0$ or $\leqslant 0$ according as $m+k$ is odd or even.

Proof : (1) follows directly from the defination of μ_k

If $k \leqslant V(\eta) \leqslant m$, then $V(\eta) \leqslant m$ for every $\mathfrak{n}|\eta$, so we have

$\theta_k(\eta, m) = \sum\limits_{\substack{\mathfrak{n}|\eta \\ V(\mathfrak{n}) \leq m}} \mu_k(\mathfrak{n}) = \sum\limits_{\mathfrak{n}|\eta} \mu_k(\mathfrak{n}) = 0$, which proved (2)

If $k \leqslant m < V(\eta)$. Let P' be the product of k distinct prime divisors of η, then

$$\theta_k(\eta, m) = \sum_{\substack{\mathfrak{n}|\eta \\ V(\mathfrak{n}) \leq m}} \mu_k(\mathfrak{n}) = \sum_{\substack{\mathfrak{b}|\eta/P' \\ V(\mathfrak{b}) \leq m}} \sum_{\substack{\mathfrak{t}|P' \\ V(\mathfrak{t}) \leq m - V(\mathfrak{b})}} \mu_k(\mathfrak{b}\mathfrak{t})$$

$$= \sum_{\substack{\mathfrak{b}|\eta/P' \\ V(\mathfrak{b}) \leq m}} (-1)^{k-1} \mu(\mathfrak{b}) \sum_{\substack{\mathfrak{t}|P' \\ V(\mathfrak{t}) \leq m - V(\mathfrak{b})}} \mu(\mathfrak{t}) \binom{V(\mathfrak{b}\mathfrak{t})-1}{k-1}$$

$$= \sum_{\substack{\mathfrak{b}|\eta/P' \\ V(\mathfrak{b}) \leq m}}{}' (-1)^{k-1} \mu(\mathfrak{b}) \sum_{i=0}^{m-V(\mathfrak{b})} \binom{k}{i} (-1)^i \binom{V(\mathfrak{b})+i-1}{k-1}$$

$$= \sum_{\substack{\mathfrak{b}|\eta/P' \\ V(\mathfrak{b}) \leq m}}{}' (-1)^{k+m-1} \sum_{i=0}^{m-V(\mathfrak{b})} (-1)^{m-V(\mathfrak{b})-i} \binom{k}{i} \binom{V(\mathfrak{b})+i-1}{k-1}$$

$\mathfrak{b}$ square free

The inner sum is $\geqslant 0$, hence we have

$$\theta_k(\mathfrak{q},\mathfrak{m}) \geqslant 0 \text{ , if } k+m \text{ is odd}$$

and

$$\theta_k(\mathfrak{q},\mathfrak{m}) \leqslant 0 \text{ , if } k+m \text{ is even}$$

Choosing m so that $k+m$ is even, then

$$\sum_{\substack{0<\xi\leq x\\ 0<\xi'\leq x'}} \sum_{\substack{\mathfrak{q}\mid \mathfrak{a}(\xi)\\ V(\mathfrak{q})\leq m-1}} \mu_k(\mathfrak{q}) \leq {}^{*}\!\mathcal{A}_k \leq \sum_{\substack{0<\xi\leq x\\ 0<\xi'\leq x'}} \sum_{\substack{\mathfrak{q}\mid \mathfrak{a}(\xi)\\ V(\mathfrak{q})<m}} \mu_k(\mathfrak{q})$$

by lemma 4. The main term of ${}^{\#}\!\mathcal{A}_k$ is

$$\frac{xx'}{\sqrt{d}} \sum_{\mathfrak{q}\mid \mathfrak{p}} \frac{\mu_k(\mathfrak{q})}{N\mathfrak{q}}$$

Now

$$\sum_{\substack{\mathfrak{q}\mid \mathfrak{p}\\ V(\mathfrak{q})<m}} \frac{\mu_k(\mathfrak{q})}{N\mathfrak{q}} = \sum_{\mathfrak{q}\mid \mathfrak{p}} \frac{\mu_k(\mathfrak{q})}{N\mathfrak{q}} \sum_{\mathfrak{n}\mid \mathfrak{q}} \mu_m(\mathfrak{n})$$

by lemma 2. Therefore, by a well-known calculation, we have

$$\sum_{\substack{\mathfrak{q}\mid P\\ V(\mathfrak{q})<m}} \frac{\mu_k(\mathfrak{q})}{N\mathfrak{q}} = \sum_{\mathfrak{n}\mid P} \frac{\mu_m(\mathfrak{n})\mu(\mathfrak{n})}{NP} \sum_{i=1}^{k} (-1)^{k-i} \binom{V(\mathfrak{n})}{k-i} \varphi_i\left(\frac{P}{\mathfrak{n}}\right)$$

$$= \frac{\varphi(P)}{NP} \sum_{\mathfrak{n}\mid P} \frac{\mu_m(\mathfrak{n})\mu(\mathfrak{n})}{\varphi(\mathfrak{n})} \sum_{i=1}^{k} (-1)^{k-i} \binom{V(\mathfrak{n})}{k-i} \left\{1+T_1\left(\frac{P}{\mathfrak{n}}\right) + \cdots + T_{i-1}\left(\frac{P}{\mathfrak{n}}\right)\right\}$$

with $T_i(\mathfrak{n}) = \sum_{\mathfrak{b}}^{*} \frac{1}{\varphi(\mathfrak{b})}$, where the star on the summation denotes that $\mathfrak{b}$ runs through the products of i distinct prime factors of $\mathfrak{n}$.

For $k=1$, we have

$$\sum_{\substack{\mathfrak{q}\mid P\\ V(\mathfrak{q})<m}} \frac{\mu_k(\mathfrak{q})}{N\mathfrak{q}} = \frac{\varphi(P)}{NP} \sum_{\mathfrak{n}\mid P} \frac{\mu_m(\mathfrak{n})\mu(\mathfrak{n})}{\varphi(\mathfrak{n})} = W(z) \sum_{\mathfrak{n}\mid P} \frac{\mu_m(\mathfrak{n})\mu(\mathfrak{n})}{\varphi(\mathfrak{n})}$$

where $W(z) = \prod_{N\mathfrak{p}<z} \left(1-\frac{1}{N\mathfrak{p}}\right)$

For $k=2$, we have

$$\sum_{\substack{\mathfrak{q}|P \\ V(\mathfrak{q})\;m}} \frac{\mu_k(\mathfrak{q})}{N\mathfrak{q}} = \frac{\varphi(P)}{NP}\sum_{\mathfrak{n}|P}\frac{\mu_m(\mathfrak{n})\mu(\mathfrak{n})}{\varphi(\mathfrak{n})}\left(1+T_1\left(\frac{P}{\mathfrak{n}}\right)-V(\mathfrak{n})\right)$$

$$=W(z)\sum_{\mathfrak{n}|P}\frac{\mu_m(\mathfrak{n})\mu(\mathfrak{n})}{\varphi(\mathfrak{n})}\left(1+T(z)-T_{\mathfrak{n}}-V(\mathfrak{n})\right)$$

$$=W(z)(1+T(z))\sum_{\mathfrak{n}|P}\frac{\mu_m(\mathfrak{n})\mu(\mathfrak{n})}{\varphi(\mathfrak{n})}-W(z)\sum_{\mathfrak{n}|P}\frac{\mu_m(\mathfrak{n})\mu(\mathfrak{n})}{\varphi(\mathfrak{n})}L_{\mathfrak{n}}$$

where $T(z)=\sum_{N\mathfrak{p}\leqslant z}\frac{1}{N\mathfrak{p}-1}$, $T_n=\sum_{\mathfrak{p}|\mathfrak{n}}\frac{1}{N\mathfrak{p}-1}$, $L_{\mathfrak{n}}'=\sum_{\mathfrak{p}|\mathfrak{n}}\frac{N\mathfrak{p}}{N\mathfrak{p}-1}$

Now following Halberstam and Richert ([1], pp48-50) we have, for $\log z \leqslant \sqrt{\log xx'}$,

$$\frac{xx'}{\sqrt{d}}\sum_{\substack{\mathfrak{q}|P \\ V(\mathfrak{q})<m}}\frac{\mu_k(\mathfrak{q})}{N\mathfrak{q}}=\frac{xx'}{\sqrt{d}}W(z)T(z)\{1+0(e^{-\sqrt{\log xx'}})\}$$

The error term of $\#\mathcal{A}_K$ is evidently $0(\sqrt{xx'})$, so we have proved

Theorem 1: If $z\geqslant 3$, $\log z\leqslant\sqrt{\log xx'}$, α is an integer in K and $\mathcal{A}_1=\{\xi;0<\xi\leqslant x, 0<\xi\leqslant x', (\xi-\alpha, P(z))=1\}$, then

$$\#\mathcal{A}_1=\frac{xx}{\sqrt{d}}W(z)\{1+0(e^{-\sqrt{\log xx'}})\}+0(\sqrt{xx'})$$

and

Theorem 2: If $z\geqslant 3$, $\log z\leqslant\sqrt{\log xx'}$, α is an integer in K, and $\mathcal{A}_2=\{\xi;\ 0<\xi\leqslant x,\ 0<\xi'\leqslant x'$, and $\xi-\alpha$ has at most one prime factor $\mathfrak{p}$ with $N\mathfrak{p}<z\}$, then

$$\#\mathcal{A}_2=\frac{xx'}{\sqrt{d}}W(z)T(z)\{1+0(e^{-\sqrt{\log xx'}})\}+0(\sqrt{xx'})$$

References

1. H. Halberstam and H. -E. Richert, "Sieve Methods", Academic Press, New York / London 1974.
2. E. Hecke, "Vörlesung über die Theorie der algebraischen Zahlen", Chelsea Publishing Company, Bronx, New York 1970.
3. D. Hensley, An Almost-Prime Sieve, J. Number Theory 10(1978), 250-262.