On smooth ideals in number fields

Johannes A. Buchmann, Christine S. Hollinger *
FB 14 - Informatik
Universität des Saarlandes
Postfach 1150
66041 Saarbrücken
Germany

11th November 1993

Abstract

For $y \in \mathbb{R}_{>0}$ an integral ideal of an algebraic number field $\mathcal{F}$ is called *y–smooth* if the norms of all of its prime ideal factors are bounded by y. Assuming the generalized Riemann hypothesis we prove a lower bound for the number $\psi_{\mathcal{F}}(x,y)$ of integral y–smooth ideals in $\mathcal{F}$ whose norms are bounded by $x \in \mathbb{R}_{>0}$. Apart from x and y this bound only depends on the degree of $\mathcal{F}$.

1 Introduction and result

Let $\mathcal{F}$ be an algebraic number field of discriminant $\Delta_{\mathcal{F}}$. For $y \in \mathbb{R}_{>0}$ an integral ideal of $\mathcal{F}$ is called *y–smooth* if the norms of all of its prime ideal factors are bounded by y. The number of integral y–smooth ideals of $\mathcal{F}$ whose norms do not exceed $x \in \mathbb{R}_{>0}$ is denoted by $\psi_{\mathcal{F}}(x,y)$. In this paper we prove the following result.

1. Theorem *Assume that the Generalized Riemann Hypothesis (GRH) is correct. For any $n \in \mathbb{N}$ and for any $\epsilon \in \mathbb{R}_{>0}$ there is an effectively computable constant $x_0(\epsilon, n) \in \mathbb{R}_{>0}$ such that for any $x, y \in \mathbb{R}_{>0}$ with*

$$x > x_0(\epsilon, n)$$

and for every algebraic number field $\mathcal{F}$ of degree n satisfying

$$\max\{(\log x)^{1+\epsilon}, (\log|\Delta_{\mathcal{F}}|)^{2+\epsilon}\} \leq y \leq \exp\left((\log x)^{1-\epsilon}\right) \tag{1}$$

*Research supported by the Deutsche Forschungsgemeinschaft

the following inequality holds:

$$\psi_{\mathcal{F}}(x,y) \geq x \cdot \exp\left(-u \cdot \left(\log u + \log\log u + O\left(\frac{1}{\epsilon} + \log \tilde{n}\right)\right)\right), \tag{2}$$

where $u = \frac{\log x}{\log y}$ *and* $\tilde{n}$ *is the degree of the normal closure of* $\mathcal{F}$ *over* $\mathbb{Q}$.

For $\mathcal{F} = \mathbb{Q}$ this result was proved by Pomerance [5]. It was generalized to imaginary quadratic fields $\mathcal{F}$ by Seysen [6], [7] see also Lenstra and Pomerance [3]. Our theorem can be used to analyze the complexity of the probabilistic class group and regulator algorithm, which was presented in [1].

Hazlewood [2] and others obtained results which look similar to Theorem 1. In those statements, however, the number field is fixed whereas in our theorem the estimates only depend on the degree of the normal closure of the number field.

2 The proof

Let $\epsilon, x, y \in \mathbb{R}_{>0}$, $n \in \mathbb{N}$ and let $\mathcal{F}$ be an algebraic number field of degree n satisfying the conditions of Theorem 1. Let $\mathcal{N}$ be the normal closure of $\mathcal{F}$. A prime number p is *totally decomposed* in $\mathcal{N}$ if it is unramified in $\mathcal{N}$ and all prime ideals of $\mathcal{N}$ lying over p have norm p. Let $\mathcal{P}$ be the set of all those totally decomposed prime numbers. Count by $\psi_{\mathcal{P}}(x,y)$ the number of positive rational integers $\leq x$ whose prime factors do not exceed y and all belong to $\mathcal{P}$. Then we get a lower bound for $\psi_{\mathcal{F}}(x,y)$ by the following result.

2. Lemma $\psi_{\mathcal{F}}(x,y) \geq \psi_{\mathcal{P}}(x,y)$.

Proof: For each prime number $p \in \mathcal{P}$ there is a prime ideal of norm p in $\mathcal{N}$ and therefore there is a prime ideal $\wp(p)$ of norm p in $\mathcal{F}$. Let a be an integer counted by $\psi_{\mathcal{P}}(x,y)$. Let

$$a = \prod_{p \in \mathcal{P}} p^{e_p}$$

be the prime number decomposition of a. Then

$$A(a) = \prod_{p \in \mathcal{P}} \wp(p)^{e_p}$$

is an integral ideal of $\mathcal{F}$, which is counted by $\psi_{\mathcal{P}}(x,y)$. The assertion follows from the fact that the map $a \mapsto A(a)$ is injective. ■

We will now prove a lower bound for $\psi_{\mathcal{P}}(x,y)$.
Let $u = \frac{\log x}{\log y}$ as in Theorem 1. From (1) it follows that $\log u \geq \log\log x - (1-\epsilon)\log\log x$. Choose $x_1 = x_1(\epsilon)$ such that $\log u \geq 3$ for every $x \geq x_1$. Define

$$w_1 = y^{1-\frac{2}{3\log u}}, \qquad w_2 = y^{1-\frac{1}{3\log u}}. \tag{3}$$

For a real number r we denote by $[r]$ be the integral part of r and we set

$$\mathcal{M} = \{m \in \mathbb{N} \mid \text{m has exactly } [u] \text{ prime factors } p \in \mathcal{P} \text{ with } \sqsupset_\infty < \surd \leq \sqsupset_\in\}. \tag{4}$$

Then we conclude as Pomerance in [5]:

3. Lemma $\psi_{\mathcal{P}}(x, y) \geq \sum_{m \in \mathcal{M}} \psi_{\mathcal{P}}(\frac{x}{m}, w_1)$.

Let m be any element of $\mathcal{M}$. We proceed by giving a lower bound for $\psi_{\mathcal{P}}(\frac{x}{m}, w_1)$. We set

$$u(m) = 1 + \left[\frac{\log(x/m)}{\log w_1}\right], \qquad w(m) = \left(\frac{x}{m}\right)^{1/u(m)}$$

and get by [7]

$$u(m) \leq \frac{u}{\log u} \cdot \left(1 + O\left(\frac{1}{\log u}\right)\right), \qquad w(m) \leq w_1. \tag{5}$$

For $w \in \mathbb{R}_{>0}$ let

$$\pi_{\mathcal{P}}(w) = \sharp\{p \in \mathcal{P} \mid \surd \leq \sqsupset\}.$$

As in [5] one can prove the following result.

4. Lemma *There exists a computable constant $x_2 = x_2(\epsilon)$ such that*

$$\psi_{\mathcal{P}}\left(\frac{x}{m}, w_1\right) \geq \left(\frac{\pi_{\mathcal{P}}(w(m))}{u(m)}\right)^{u(m)}$$

for every $x > x_2$.

Next, we prove a lower bound for $\pi_{\mathcal{P}}(w(m))$. As in Theorem 1 we denote by $\tilde{n}$ the degree of the normal closure $\mathcal{N}$ of $\mathcal{F}$ over $\mathbb{Q}$.

5. Lemma *Assume that the GRH is correct. Then for any $\delta \in \mathbb{R}_{>0}$ there is a computable constant $w_1 = w_1(\delta, n) > 0$ such that*

$$\pi_{\mathcal{P}}(w) \geq \frac{1}{2\tilde{n}} \cdot \frac{w}{\log w}$$

for every $w \in \mathbb{R}_{>0}$ with $w \geq \max\{w_1, (\log|\Delta_{\mathcal{F}}|)^{2+\delta}\}$.

Proof: By a result of Oesterlé [4] we have for any $w \in \mathbb{R}_{\geq 2}$

$$\left|\pi_{\mathcal{P}}(w) - \frac{1}{\tilde{n}} \cdot Li(w)\right| \leq \frac{1}{\tilde{n}}\sqrt{w} \cdot (2\log|\Delta_{\mathcal{N}}| + \tilde{n}\log w)$$

where $Li(w) = \int_2^w \frac{1}{\log t}\, dt$ is the *logarithmic integral.* Applying the mean value theorem to $Li(w)$ and using $\Delta_{\mathcal{N}} \mid \Delta_{\mathcal{F}}^{\tilde{n}}$ (see [8]) we obtain

$$\pi_{\mathcal{P}}(w) \geq \frac{1}{\tilde{n}} \cdot \left(\frac{w-2}{\log w} - \tilde{n}\sqrt{w} \cdot (2\log|\Delta_{\mathcal{F}}| + \log w)\right).$$

If $w \geq (\log|\Delta_{\mathcal{F}}|)^{2+\delta}$ then $\log|\Delta_{\mathcal{F}}| \leq w^{1/(2+\delta)}$ and therefore

$$\pi_{\mathcal{P}}(w) \geq \frac{1}{\tilde{n}} \cdot \left(\frac{w-2}{\log w} - 2\tilde{n}w^{1/2+1/(2+\delta)} - \tilde{n}w^{1/2}\log w\right).$$

From this inequality we can immediately deduce the assertion. ■

6. Lemma *There are computable constants $x_3 = x_3(\epsilon, n)$ and $c \in \mathbb{R}_{>0}$ such that*

$$\psi_{\mathcal{P}}(x,y) \geq x \cdot \exp\left(-u \cdot c\left(\frac{1}{\epsilon} + \log(2\tilde{n})\right)\right) \cdot \sum_{m \in \mathcal{M}} \frac{1}{m}$$

for every $x > x_3$.

Proof: We apply arguments similar to those used in [7]. It is easy to see that $x \to \infty$ implies $w(m) \to \infty$. Therefore, by (5), Lemma 4 and Lemma 5 there is a computable constant $x_4 = x_4(\epsilon, n)$ such that for $x > x_4$

$$\begin{aligned}
\psi_{\mathcal{P}}\left(\frac{x}{m}, w(m)\right) &\geq \left(\frac{w(m)}{2\tilde{n} \cdot \log w(m) \cdot u(m)}\right)^{u(m)} \\
&= \frac{x}{m} \cdot \exp\left(-u(m) \cdot (\log u - \log\log u + \log\log y + \log\tilde{n} + O(1))\right).
\end{aligned}$$

From (1) and the definition of u we deduce

$$\log\log y \leq \frac{1-\epsilon}{\epsilon}\log u$$

and conclude that

$$\psi_{\mathcal{P}}\left(\frac{x}{m}, w(m)\right) \geq \frac{x}{m} \cdot \exp\left(-u(m) \cdot \left(\frac{1}{\epsilon} \cdot \log u - \log\log u + \log\tilde{n} + O(1)\right)\right).$$

Also, we have $\log\log u \geq 0$ for $x > x_1$, as we saw above. Therefore

$$\psi_{\mathcal{P}}\left(\frac{x}{m}, w(m)\right) \geq \frac{x}{m} \cdot \exp\left(-u(m) \cdot \log u \cdot \left(\frac{1}{\epsilon} + \log\tilde{n} + O(1)\right)\right)$$

for all $x > x_5$ with some computable $x_5 = x_5(\epsilon, n)$. With (5) we finally find that there exists a computable constant $c \in \mathbb{R}_{>0}$ such that for all $x > x_5$

$$\psi_{\mathcal{P}}(x,y) \geq x \cdot \exp\left(-u \cdot c\left(\frac{1}{\epsilon} + \log\tilde{n}\right)\right) \cdot \sum_{m \in \mathcal{M}} \frac{1}{m}. \tag{6}$$

■

To finish the proof of Theorem 1 it remains to show a lower bound for $\sum_{m\in\mathcal{M}} \frac{1}{m}$ in (6).

7. Lemma *Assume that the GRH is correct. There exists a computable constant $x_6 = x_6(\epsilon, n)$ such that*

$$\sum_{m\in\mathcal{M}} \frac{1}{m} \geq \exp\left(-u\cdot(\log u + \log\log u + \log(5\tilde{n}))\right)$$

for all $x > x_6$.

Proof: Using the definition of $\mathcal{M}$ in (4) we obtain

$$\sum_{m\in\mathcal{M}} \frac{1}{m} \geq \frac{1}{[u]!}\left(\sum_{w_1<p\leq w_2, p\in\mathcal{P}} \frac{1}{p}\right)^{[u]}.$$

By arguments of Seysen [7] it can be shown that for $x > x_7$ for some computable $x_7 = x_7(\epsilon, n)$ there exists $\epsilon_1 \in \mathbb{R}_{>0}$ such that

$$\sum_{w_1<p\leq w_2, p\in\mathcal{P}} \frac{1}{p} \geq \frac{1}{\tilde{n}}\cdot(\log\log w_2 - \log\log w_1) - O(w_1^{-\epsilon_1}).$$

Applying the definition of $w_1,\ w_2$ in (3) this implies that for $x > x_8 = x_8(\epsilon, n)$

$$\sum_{m\in\mathcal{M}} \frac{1}{m} \geq \exp\left(-u\cdot(\log u + \log\log u + \log(5\tilde{n}))\right).$$

■

Combining Lemma 3, 6 and 7 we obtain the assertion of Theorem 1.

References

[1] J. Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Séminaire de théorie des nombres, Paris 1988 - 1989, 28 - 41.

[2] D. G. Hazlewood, *On ideals having only small prime factors*, Rocky Mountain Journal of Mathematics, **7**, (1977), 753 - 768.

[3] H.W. Lenstra jr. and C. Pomerance, *A rigorous time bound for factoring integers*, J. American Math. Society, **5**, (1992), 483–516.

[4] J. Oesterlé, *Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée*, Société mathématique de France, Astérisque **61**, (1979), 165–167.

[5] C. Pomerance, *Analysis and comparison of some integer factoring algorithms*, Computational methods in number theory I, edited by H.W. Lenstra & R. Tijdeman, Math. Centre Tracts, 1987, 89 - 140.

[6] M. Seysen, *A probabilistic factorization algorithm with quadratic forms of negative discriminant*, Math. Comp., **48**, (1987), 757–780.

[7] M. Seysen, *Ein probabilistischer Faktorisierungsalgorithmus mit quadratischen Formen negativer Diskriminante*, Dissertation, Universität Frankfurt am Main, 1984.

[8] H.M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Inventiones math. **23**, (1974), 135–152.