JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

VOLKER KESSLER

# On the minimum of the unit lattice

*Journal de Théorie des Nombres de Bordeaux 2e série*, tome 3, nº 2 (1991), p. 377-380

<http://www.numdam.org/item?id=JTNB_1991__3_2_377_0>

*Séminaire de Théorie des Nombres,*
*Bordeaux* **3** *(1991), 377-380*

# On the minimum of the unit lattice.

PAR VOLKER KESSLER

## 1. Introduction.

Computations in lattices often require a lower bound for the minimum of the lattice, both for practical purposes and for a theoretical analysis of the algorithms, e.g. [1] and [2].

In this paper we recall two results of Dobrowolski [3] and Smyth [5] in order to get such a bound for the unit lattice.

## 2. Lower bound.

Let $K$ be a finite extension of $\mathbb{Q}$ of degree $n$ with maximal order $R$. For $1 \leq i \leq n$ we denote by

$$K \to K^{(i)} \subset \mathbb{C}, \quad \alpha \to \alpha^{(i)}$$

the $n$ different embeddings of $K$ into the field $\mathbb{C}$ of complex numbers. The first $r_1$ of those embeddings are real, the last $2r_2$ embeddings are non-real and numbered such that the $(r_1 + r_2 + i)$th embedding is the complex-conjugation of the $(r_1 + i)$th embedding. Then the logarithmic map is given by

$$\mathrm{Log} : K^* \to \mathbb{R}^r, \quad \mathrm{Log}(\alpha) := (c_1 \log |\alpha^{(1)}|, \cdots, c_r \log |\alpha^{(r)}|)$$

with the unit rank $r = r_1 + r_2 - 1$ and

$$c_i = \begin{cases} 1 & \text{for } 1 \leq i \leq r_1 \\ 2 & \text{for } r_1 + 1 \leq i \leq r + 1. \end{cases}$$

The kernel of Log consists exactly of the roots of the unity lying in $K$. We define the *minimum* $\lambda(L)$ of the *unit lattice* $L := Log(R^*)$ by

$$\lambda(L) = \min\{ \, ||v|| \; | v \in L \backslash \{0\}\}$$

Manuscrit reçu le 8 février 1991.

where $|| \ ||$ denotes the Euclidean norm.

THEOREM : *A lower bound for the minimum* $\lambda(L)$ *is given by*

(1)
$$\lambda(L) > \mu(K) := \sqrt{\frac{2}{r+1}}\left(\frac{1}{1200}(\frac{\log\log n}{\log n})^3 - \frac{1}{2880000}(\frac{\log\log n}{\log n})^6\right)$$

*which is "a bit" larger than*

$$\frac{1}{\sqrt{r+1}}\frac{1}{1000}(\frac{\log\log n}{\log n})^3.$$

*Thus the inverse* $1/\lambda(L)$ *is of the magnitude* $0(n^{1/2+\epsilon})$ *for every* $\epsilon > 0$.

PROOF. Let $\epsilon \in R^*$ be a unit of degree $m$ over $\mathbb{Q}$, which is no root of unity. Without loss of generality we can assume that $m = n$, because if $||\mathrm{Log}\ \epsilon||$ is larger than $\mu(K')$ for a subfield $K'$ of $K$ it is also larger than $\mu(K)$.

We are interested in two subsets of the conjugates $\epsilon^{(1)}, \cdots, \epsilon^{(n)}$

$$S := \{1 \le i \le r+1 \mid |\epsilon^{(i)}| > 1\}$$
$$T := \{1 \le i \le r+1 \mid |\epsilon^{(i)}| < 1\}.$$

Since $\epsilon$ is no root of unity $S$ is non-empty and therefore $T$ cannot be empty because of $N(\epsilon) = 1$.

We call $\epsilon$ *reciprocal* if $\epsilon$ is conjugate to $\epsilon^{-1}$, i.e. its minimal polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ satisfies

$$f(X) = X^n f(\frac{1}{X}) = a_0 X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + 1.$$

If $\epsilon$ is <u>non-reciprocal</u> we know from the theorem of [5] that

$$\prod_{i \in S} |\epsilon^{(i)}|^{c_i} \ge \theta$$

where $\theta$ is the real root of $X^3 - X - 1$, i.e. $\theta \approx 1.3247$. Thus

(2)
$$\sum_{i \in S} c_i \log|\epsilon^{(i)}| \ge \log\theta \approx 0.281$$

But from $N(\epsilon) = 1$ it follows

$$\sum_{i \in S} c_i \log |\epsilon^{(i)}| = -\sum_{i \in T} c_i \log |\epsilon^{(i)}|. \tag{3}$$

The value $c_{r+1} \log |\epsilon^{(r+1)}|$ does not occur in the norm of $\mathrm{Log}(\epsilon)$. But as a consequence of (3) it does not matter if $r+1$ lies in $S$ or in $T$ and so we can assume without restriction that $r+1 \notin S$. Thus

$$\begin{aligned} ||\mathrm{Log}(\epsilon)|| &\geq \sqrt{\sum_{i \in S} (c_i \ \log |\epsilon^{(i)}|)^2} \\ &\geq r^{-1/2} \sum_{i \in S} (c_i \ \log |\epsilon^{(i)}|) \geq r^{-1/2} \log \ \theta > \mu(K). \end{aligned}$$

(The second inequality follows from the well known norm equivalence between 1-norm and Euclidean norm.)

For <u>reciprocal</u> $\epsilon$ we know by Theorem 1 of [3] :

$$\prod_{i \in S} |\epsilon^{(i)}|^{c_i} > 1 + \frac{1}{1200} \left(\frac{\log \ \log \ n}{\log \ n}\right)^3. \tag{4}$$

We now use the Taylor series of the logarithm ($|y| < 1$) :

$$\log(1 + y) = y - \frac{y^2}{2} + \frac{y^3}{3} \mp \cdots > y - \frac{y^2}{2}. \tag{5}$$

The inequality follows directly from Lagrange's representation of the residue. Applying (5) to (4) yields

$$\sum_{i \in S} c_i \ \log |\epsilon^{(i)}| > \frac{1}{1200} \left(\frac{\log \log n}{\log n}\right)^3 - \frac{1}{2880000} \left(\frac{\log \log n}{\log n}\right)^6.$$

Since $\epsilon$ is reciprocal the inverses of the conjugates of $\epsilon$ are also conjugate to $\epsilon$. This implies that the numbers of conjugates outside the unit circle equals the number of conjugates inside the unit circle, i.e

$$\#S = \#T \leq \frac{r+1}{2} \leq \frac{n}{2}.$$

Again by (3) we can assume that $r+1 \notin S$

$$||\mathrm{Log}(\epsilon)|| \geq \sqrt{\sum_{i \in S}(c_i \log |\epsilon^{(i)}|)^2} \geq \sqrt{\frac{2}{r+1}} \sum_{i \in S} c_i \log |\epsilon^{(i)}|$$

$$> \sqrt{\frac{2}{r+1}} \left( \frac{1}{1200} (\frac{\log \log n}{\log n})^3 - \frac{1}{2880000} (\frac{\log \log n}{\log n})^6 \right) = \mu(K)$$

which is larger than

$$\sqrt{\frac{2}{r+1}} (\frac{1}{1200} - \frac{1}{2880000})(\frac{\log \log n}{\log n})^3.$$

Because of $\sqrt{2}(\frac{1}{1200} - \frac{1}{2880000}) \approx 0.001178$ we thus proved the lower bound.

REMARK. If the conjecture of Schinzel and Zassenhaus [5] is correct the term $(\frac{\log \log n}{\log n})^3$ can be substituted by a constant independent of $n$. This bound would be provable the best one (up to constants).

## REFERENCES


[1] Buchmann, *Zur Komplexität der Berechnung von Einheiten und Klassenzahlen algebraicher Zahlkörper*, Habilitationsschrift Düsseldorf (1987).

[2] Buchmann, Kessler, *Computing a reduced lattice basis from a generating system*, to appear.

[3] Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta arithmetica **34** (1979), 391-401.

[4] Schinzel, Zassenhaus, *A refinement of two theorems of Kronecker*, Mich. Math. J. **12** (1965), 81-84.

[5] Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. **3** (1971), 169-175.



Volker Kessler
Siemens AG
ZFE ST SN 5
Otto-Hahn-Ring 6
D-8000 München 83.