ACTA ARITHMETICA
LXXXV.3 (1998)

Divisors in a Dedekind domain

by

Javier Cilleruelo and Jorge Jiménez-Urroz (Madrid)

1. Introduction. Let $\mathcal{A}$ be a Dedekind domain in which we can define a notion of distance. We are interested in the number of divisors that an element $\alpha \in \mathcal{A}$ can have in a small interval.

Of course, we cannot talk about divisors if our domain is not a UFD. Hence, the convinient object to deal with will be the ideals of $\mathcal{A}$.

We are able to prove a general theorem about the minimal length that an interval can have containing k divisors of a fixed $\mathcal{M}$ in terms of the size of these divisors.

Let φ be a real-valued function over the ideals in $\mathcal{A}$ such that

$$\text{(i)} \qquad \varphi(\alpha) \geq 0,$$

$$\text{(ii)} \qquad \varphi(\alpha\beta) = \varphi(\alpha) + \varphi(\beta),$$

and let us write (α, β) for the greatest common divisor of α and β. We prove

Theorem 1.1. *Let $\alpha_1, \ldots, \alpha_k$ be ideals in $\mathcal{A}$ with least common multiple $\mathcal{M} = [\alpha_1, \ldots, \alpha_k]$ and such that $\varphi(\alpha_i) \geq \gamma\varphi(\mathcal{N})$ for some multiple $\mathcal{N}$ of $\mathcal{M}$. If $L \in \mathbb{R}$ is such that $\varphi((\alpha_j, \alpha_i)) \leq L$ for all $1 \leq j, i \leq k$, then*

$$L \geq E_k(\gamma)\varphi(\mathcal{N})$$

where

$$E_k(\gamma) = \frac{[k\gamma](2k\gamma - [k\gamma] - 1)}{k(k-1)}.$$

Notice that $E_k(\gamma) > \gamma^2 - \gamma\left(\frac{1-\gamma}{k-1}\right)$ and that it is increasing as a function of either γ or k.

This result came out when studying lattice points on conics, and this is in fact our principal application of the theorem.

1991 *Mathematics Subject Classification*: 11R04, 11A05.

By means of the identity $N=(x+y\sqrt{d})(x-y\sqrt{d})$, valid for any lattice point, (x,y), on the conic, and introducing the quadratic field $\mathbb{Q}(\sqrt{d})$, all the problems about lattice points can be translated in terms of divisors $(x+y\sqrt{d})=\alpha\in\mathcal{A}$ of N, where $\mathcal{A}$ is the ring of integers of $\mathbb{Q}(\sqrt{d})$.

So, a first problem that appears is trying to deal with "divisors" when we are not in a unique factorization domain. This can be avoided by introducing the ideals in $\mathcal{A}$ which guarantee unique factorization. The difficulty will now be how to translate the information from ideals to the elements.

In [2] and [3], this is only possible for principal ideals. We will get information from all the ideals, by means of Theorem 1.1 and noting that in fact an ideal is, in some sense, a divisor of its elements.

In this way, we give a new proof of Theorem 1 of [1], and give improvements on the principal results of [2] and [3].

Theorem 1.2. *Let $d\neq 0,1$ be a fixed squarefree integer. On the conic $x^2-dy^2=N$, an arc of length N^α with $\alpha\le 1/4-1/(8[k/2]+4)$ contains at most k lattice points.*

In this theorem we have avoided the case $d=1$, considered in [4]. However, in this case we are able to prove the analogous result, but this time we will cover all the ranges of the hyperbola. Meanwhile as we have seen, Theorem 1.2 only includes $\gamma=1/2$ of Theorem 1.1.

The key point for the improvement in this particular case is that any lattice point on $x^2-y^2=N$ gives us another one on the hyperbola $XY=N$, with coordinates $X=x-y$, $Y=x+y$. So, looking at the latter curve, we see that each lattice point corresponds to an integral divisor $X\in\mathbb{Z}$ of N. We can prove

Theorem 1.3. *On the hyperbola $xy=N$ there are at most k lattice points $(x_1,y_1),\ldots,(x_k,y_k)$ such that $N^\gamma\le x_1<\ldots<x_k$ and $x_k-x_1\le N^{E_k(\gamma)}$.*

Finally, in order to show the more general character of Theorem 1.1, we will include an application concerning polynomials.

Theorem 1.4. *Let $F_1(x),\ldots,F_k(x)$ be polynomials in $\mathbb{Z}[x]$ with least common multiple $M(x)$ and such that $\deg(F_i(x))\ge\gamma\deg(M(x))$. Then there exist $i<j$ such that*

$$\deg(F_j(x)-F_i(x))\ge\deg(M(x))E_k(\gamma).$$

Acknowledgments. We wish to thank A. Granville for his suggestion to state Theorem 1.1 in terms of ideals directly.

2. Proofs of theorems

Proof of Theorem 1.1. For any ideal $\beta \in \mathcal{A}$ and some prime ideal π, we define $v_\pi(\beta) = t$ to be the greatest power of π dividing β.

v_π is well defined since, in a Dedekind domain, we have unique factorization of ideals. Further, we know that every ideal α has an inverse α^{-1} which is a fractional ideal. Hence, we can extend the definition of v_π and φ to the inverses of ideals in such a way that $v_\pi(\alpha^{-1}) = -v_\pi(\alpha)$, and $\varphi(\alpha^{-1}) = -\varphi(\alpha)$.

Now, let us order the ideals $\alpha_1, \ldots, \alpha_k$ so that $v_\pi(\alpha_i) = t_i$ increases with i. Then

$$v_\pi\Big(\prod(\alpha_j, \alpha_i)\Big) = \sum_{1\le i<j\le k} t_i = \sum_{i=1}^{k-1} t_i \sum_{j=i+1}^{k} 1 = \sum_{i=1}^{k} t_i(k-i),$$

and on the other hand,

$$v_\pi\Big(\prod \alpha_i\Big) = \sum_{1\le i\le k} t_i.$$

Hence, grouping all the local information on each prime, we can write

$$\prod(\alpha_j, \alpha_i) = \prod_{\pi|\mathcal{M}} \pi^{\sum_{1\le i\le k} t_i(k-i)}, \qquad \prod \alpha_i = \prod_{\pi|\mathcal{M}} \pi^{\sum_{1\le i\le k} t_i},$$

and so, for any integer m we have

$$\prod(\alpha_j, \alpha_i) = \Big(\prod \alpha_i\Big)^m \prod_{\pi|\mathcal{M}} \pi^{\sum_{1\le i\le k} t_i(k-i-m)}. \tag{2.1}$$

Now, since $k-i-m \ge 0$ when $i \le k-m$, we have

$$\begin{aligned}\sum_{1\le i\le k} t_i(k-i-m) &\ge -\sum_{k-m\le i\le k} t_i(i-(k-m))\\ &\ge -t_k \sum_{k-m\le i\le k} (i-(k-m)) = -t_k\binom{m+1}{2},\end{aligned}$$

where we have used $t_i \le t_k$. Hence, by properties (i) and (ii) of φ and looking at the identity $\mathcal{M} = \prod_{\pi|\mathcal{M}} \pi^{t_k}$, we deduce by substitution in (2.1) that

$$\binom{k}{2}L \ge \sum \varphi((\alpha_j, \alpha_i)) \ge m\sum \varphi(\alpha_i) - \binom{m+1}{2}\varphi(\mathcal{M}),$$

and so, from the hypothesis $\varphi(\alpha_i) \ge \gamma\varphi(\mathcal{N})$ and $\varphi(\mathcal{M}) \le \varphi(\mathcal{N})$ (since $\mathcal{M} \,|\, \mathcal{N}$), we get

$$\binom{k}{2}L \ge \varphi(\mathcal{N})\Big(k\gamma m - \binom{m+1}{2}\Big).$$

The proof is now concluded by choosing $m = [k\gamma]$, which maximizes the above quantity. ■

Proof of Theorem 1.4. Let us first prove Theorem 1.4, and see how Theorem 1.1 works in that context. So, consider $\mathcal{A} = \mathbb{Z}[x]$. This is a principal ideal domain and the function $\varphi(\mathcal{F}) = \deg F(x)$, which has properties (i) and (ii), is well defined, where $F(x)$ is the generator of the ideal $\mathcal{F}$. The conclusion of the theorem is now clear since $\deg(F_j(x) - F_i(x)) \geq \deg(F_j(x), F_i(x))$. ■

Proof of Theorem 1.2. Suppose we now have k lattice points $(a_1, b_1), \ldots, (a_k, b_k)$ on the conic $x^2 - dy^2 = N$, with $d \neq 0, 1$. Let $\mathcal{A}$ be the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{d})$, $\alpha_i = \langle a_i + b_i\sqrt{d}\rangle$ the ideal generated by $a_i + b_i\sqrt{d}$, and consider, for any α ideal in $\mathcal{A}$, the function $\varphi(\alpha) = \log(\mathbf{N}(\alpha))$, where $\mathbf{N}(\alpha)$ is the norm of the ideal. This function again has the properties of Theorem 1.2.

Now, since $a_i^2 - db_i^2 = N$, we have $\mathbf{N}(\alpha_i) = N$, and we find $\langle N\rangle$ to be a multiple of the least common multiple of α_i. Now, $\varphi(\langle N\rangle) = 2\log N$, and hence $\varphi(\alpha_i) = (1/2)\varphi(\langle N\rangle)$, so by Theorem 1.1,

$$\varphi((\alpha_j, \alpha_i)) \geq 2E_k(1/2)\log N. \tag{2.2}$$

On the other hand, for any $1 \leq i < j \leq k$ we clearly have $|\xi_j - \xi_i| \geq \sqrt{\mathbf{N}(\xi_j - \xi_i)}$, where $\xi_i = a_i + b_i\sqrt{d}$, and $|\xi|$ is the euclidean distance from ξ to the origin $O = 0 + 0\sqrt{d}$, and so

$$\log|\xi_j - \xi_i| \geq \tfrac{1}{2}\log(|\mathbf{N}(\xi_j - \xi_i)|) = \tfrac{1}{2}\varphi(\langle\xi_j - \xi_i\rangle).$$

Finally, we have $\langle\xi_j - \xi_i\rangle \subset \langle\alpha_j - \alpha_i\rangle$, and we know [5] that $\langle\alpha_j - \alpha_i\rangle = (\alpha_j, \alpha_i)$, so $(\alpha_j, \alpha_i) \mid \langle\xi_j - \xi_i\rangle$, and by the properties of φ and (2.2),

$$2\log|\xi_j - \xi_i| \geq \varphi(\langle\xi_j - \xi_i\rangle) \geq \varphi((\alpha_j, \alpha_i)) \geq 2E_k(1/2)\log N,$$

which ends the proof. ■

Proof of Theorem 1.3. To prove the case $d = 1$, or more concretely Theorem 1.3, we apply Theorem 1.1 to $\mathcal{A} = \mathbb{Z}$ and $\varphi(x) = \log|x|$, where x is an ideal or the element generating the ideal. So, Theorem 1.1 together with

$$\varphi(x_j - x_i) \geq \varphi((x_j, x_i))$$

gives the result. ■

References

[1] J. Cilleruelo and A. Córdoba, *Trigonometric polynomials and lattice points*, Proc. Amer. Math. Soc. 115 (1992), 899–905.

[2] —, —, *Lattice points on ellipses*, Duke Math. J. 76 (1994), 741–750.

[3] J. Cilleruelo and J. Jiménez-Urroz, *Lattice points on hyperbolas*, J. Number Theory 63 (1997), 267–274.

[4] A. Granville and J. Jiménez-Urroz, *The least common multiple and lattice points on hyperbolas*, preprint, 1995.

[5] I. N. Stewart and D. O. Tall, *Algebraic Number Theory*, Chapman and Hall, London, 1987.

Departamento de Matemáticas
Facultad de Ciencias
Universidad Autónoma de Madrid
28049 Madrid, Spain
E-mail: franciscojavier.cilleruelo@uam.es
jorge.jimenez@uam.es

Received on 10.6.1997 (3202)