Proc. Indian Acad. Sci. (Math. Sci.) Vol. 124, No. 4, November 2014, pp. 481–485.

Lenstra theorem in number fields

S SUBBURAM

Department of Mathematics, SASTRA University, Thanjavur 613 401, India
Present Address: The Institute of Mathematics, CIT Campus, Taramani, Chennai 600 113, India
E-mail: ssubburam@maths.sastra.edu; ssubburam@imsc.res.in

MS received 22 March 2013; revised 28 September 2013

Abstract. In this paper, we present a number field version of the celebrated result of Lenstra (*Math. Comp.* **42(165)** (1984) 331–340) in 1984. Also, this result allows us to improve a result of Wikstrőm (On the l-ary GCD-algorithm in rings of integers (2005) pp. 1189–1201).

Keywords. Divisors; norm; weight; principal ideal.

2000 Mathematics Subject Classification. 11R04; 11R21.

1. Introduction

In 1984, Lenstra [1] proved the following theorem:

Let r, s and n be integers satisfying

$$0 \leq r < s < n, s > n^{1/3}, \quad (r, s) = 1.$$

Then n has at most 11 *positive divisors which are congruent to r modulo s.*

This result has been applied to solve many problems. Recently, Luca and Togbe [2] and Subburam [4] applied this result on a conjecture of Mohanty and Ramasamy [3].

Let K be any number field, $\mathcal{O}_K$ its ring of integers and G the set of all $\mathbb{Q}$-embeddings of K into $\mathbb{C}$. Then we denote the norm of an element $\alpha \in K$ as

$$N(\alpha) = N_{K/\mathbb{Q}}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha).$$

Throughout this paper, we have the following notations: $\gcd(\alpha, \beta)$ is the greatest common divisor of the principal ideals $\alpha\mathcal{O}_K$ and $\beta\mathcal{O}_K$, $\mathbb{Z}$ is the set of all rational integers and the cardinality of a finite set A is $|A|$.

In this paper, we prove the following theorem.

Theorem 1. *Let $\mathcal{O}_K$ be a principal ideal domain and α be any positive real number, and let $r, s, n \in \mathcal{O}_K$ satisfying*

$$|N(n)| > 1, |N(s)| > \alpha, |N(s)| \geq \alpha |N(n)|^{1/3} \quad \text{and} \quad \gcd(r, s) = \mathcal{O}_K.$$

Then any collection $\mathcal{A} \subseteq \mathcal{O}_K$ such that

(1) *d divides n;*

(2) $d \equiv r \pmod{s}$;
(3) *if* d *is not an associate of* d', *then* $|N(d)| \neq |N(d')|$;
(4) $|N(d - d')| \leq \alpha \max\{|N(d)|, |N(d')|\}$;

for all $d, d' \in \mathcal{A}$, *has at most* 11 *elements.*

In 2005, Wikstrőm [5] mentioned that it would be nice if given $\alpha, \beta \in K$, we had

$$|N(\alpha + \beta)| \leq c \max\{|N(\alpha)|, |N(\beta)|\}$$

for a real constant c. Unfortunately, no such law exists for almost all K. In the same paper, he showed as follows:

Let α, β *be in* K *and* Δ *be a positive real number such that*

$$|\sigma_1(\alpha)|/|\sigma_2(\alpha)| \leq \Delta \quad \textit{and} \quad |\sigma_1(\beta)|/|\sigma_2(\beta)| \leq \Delta$$

for any $\sigma_1, \sigma_2 \in G$. *Then*

$$|N(\alpha + \beta)| \leq 2^{|G|} \Delta^{|G|-1} \max\{|N(\alpha)|, |N(\beta)|\}.$$

Here we prove the following theorem.

Theorem 2. *Let* α, β *be in* K *and let* Δ *be a positive real number such that*

$$0 < \theta(\alpha) \leq \Delta \min\{\sigma(\alpha) : \sigma \in G\} \quad \textit{and} \quad 0 < \theta(\beta) \leq \Delta \min\{\sigma(\beta) : \sigma \in G\}$$

for all $\theta \in G$. *Then*

$$|N(\alpha - \beta)| \leq \Delta^{|G|-1} \max\{N(\alpha), N(\beta)\}.$$

Finally, we prove the following.

Theorem 3. *Let* $\mathcal{O}_K$ *be a principal ideal domain and* Δ *be any positive real number, and let* $r, s, n \in \mathcal{O}_K$ *satisfying*

$$|N(n)| > 1, |N(s)| > \Delta^{|G|-1}, |N(s)| \geq \Delta^{|G|-1} |N(n)|^{1/3}, \gcd(r, s) = \mathcal{O}_K.$$

Then any collection $\mathcal{A} \subseteq \mathcal{O}_K$ *such that*

(1) d *divides* n;
(2) $d \equiv r \pmod{s}$;
(3) *if* d *is not an associate of* d', *then* $|N(d)| \neq |N(d')|$;
(4) *for all* $\sigma \in G$, $\sigma(d)$ *is real with* $0 < \sigma(d) \leq \Delta \min\{\delta(d) : \delta \in G\}$;

for all $d, d' \in \mathcal{A}$, *has at most* 11 *elements.*

2. Preliminaries

In this section, the difference of any two sets A and B is denoted by $A - B$. We write the following lemma from the proof of Proposition 2.4 in [1].

Lemma 1. *Let* V *be a finite set,* w *be a weight function on* V *with* $w(V) > 0$, *and* $\alpha > 1/4$ *be real. Let* $\mathcal{D}$ *be a system of subsets of* V *such that*

$$\max\{w(D - D'), w(D' - D)\} \geq \alpha w(V)$$

for all $D, D' \in \mathcal{D}$ with $D \neq D'$. Let $V_1, V_2, \ldots, V_{12} \in \mathcal{D}$ be distinct with

$$w(V_1) \leq w(V_2) \leq \cdots \leq w(V_{12}).$$

Then the numbers $x_i = w(V_i)/w(V)$ satisfy the inequality

$$x_5 - x_6 + x_7 - x_8 + 12 \geq 36\alpha.$$

Lemma 2. *Let $\alpha \geq 1/3$, V, w and $\mathcal{D}$ be defined as in Lemma* 1. *If*

$$w(D) \neq w(D')$$

for any $D, D' \in \mathcal{D}$ with $D \neq D'$, then

$$\#\mathcal{D} \leq 11.$$

Proof. Suppose that $\#\mathcal{D} \geq 12$. Then there exist distinct elements $D_1, D_2, \ldots, D_{12}$ in $\mathcal{D}$ such that

$$w(D_1) \leq w(D_2) \leq \cdots \leq w(D_{12}).$$

So, by Lemma 1, the numbers

$$x_i = \frac{w(D_i)}{w(V)}$$

satisfy the inequality

$$x_5 - x_6 + x_7 - x_8 + 12 \geq 36\alpha. \tag{1}$$

Since $w(D) \neq w(D')$ for any $D, D' \in \mathcal{D}$ with $D \neq D'$, we have

$$\min\{|w(D) - w(D')| : D, D' \in \mathcal{D} \text{ with } D \neq D'\}/w(V) > 0.$$

Therefore

$$x_i = \frac{w(D_i)}{w(V)} = \frac{w(D_{i-1})}{w(V)} + \frac{(w(D_i) - w(D_{i-1}))}{w(V)} > \frac{w(D_{i-1})}{w(V)} = x_{i-1}$$

for any $i \geq 2$. From this, we conclude that

$$x_6 > x_5 \quad \text{and} \quad x_8 > x_7.$$

Therefore, by (1), we obtain $\alpha < 1/3$ which is a contradiction. This proves the lemma. □

3. Proof of Theorem 1

Let m be any divisor of n. Then we define

$$V(m) = \{(p\mathcal{O}_K)^t : p \text{ is prime in } \mathcal{O}_K, t \in \mathbb{Z}, t > 0,\ p^t \mid m\},$$

and a weight w on $V(m)$ by taking $w(\{(p\mathcal{O}_K)^t\}) = \log|N(p)|$. In this way, by the conditions of weight function, we have $w(V(m)) = \log|N(m)|$, since $\mathcal{O}_K$ is a principal ideal domain. Let

$$\mathcal{D} = \{V(d) : d \mid n\}$$

be such that for any distinct $V(d)$ and $V(d')$ in $\mathcal{D}$, there exist two units u and u' in $\mathcal{O}_K$ satisfying $ud \equiv r \pmod{s}$, $u'd' \equiv r \pmod{s}$, $|N(d)| \neq |N(d')|$ and

$$|N(ud - u'd')| \leq \alpha \max\{|N(ud)|, |N(u'd')|\}.$$

First we shall prove that $|\mathcal{A}| \leq |\mathcal{D}|$. Let d and d' be distinct elements of $\mathcal{A}$. If d is an associate of d', then $d' = ud$ for some unit $u \neq 1$ in $\mathcal{O}_K$. Since $\gcd(r, s) = \mathcal{O}_K$, $d \equiv r \pmod{s}$ and $d' = ud \equiv r \pmod{s}$, $s \mid (u - 1)$ and so $|N(s)| \leq |N(u - 1)|$. Also $|N(d - ud)| \leq \alpha \max\{|N(d)|, |N(ud)|\}$ implies that $|N(u - 1)| \leq \alpha$. Therefore we have $|N(s)| \leq \alpha$ which is a contradiction to $|N(s)| > \alpha$. This tells that $V(d) \neq V(d')$. This proves the claim.

Let $V(d), V(d') \in \mathcal{D}$ be distinct. To prove the theorem, by Lemma 2 and the above result, it is enough to prove that

(i) $w(V(n)) > 0$,
(ii) $w(V(d)) \neq w(V(d'))$,
(iii) $\max\{w(V(d) - V(d')), w(V(d') - V(d))\} \geq (1/3)w(V(n))$.

Since $|N(n)| > 1$, $w(V(n)) = \log|N(n)| > 0$. So (i) is true. Since $|N(d)| \neq |N(d')|$, $\log|N(d)| \neq \log|N(d')|$. This proves (ii). Finally, we shall prove (iii). Without loss of generality, we shall assume that $d \equiv r \pmod{s}$, $d' \equiv r \pmod{s}$ and

$$|N(d - d')| \leq \alpha \max\{|N(d)|, |N(d')|\}. \tag{2}$$

Then we have $s \mid (d - d')$. Since $\gcd(r, s) = \mathcal{O}_K$, $\gcd(d, s) = \gcd(d', s) = \mathcal{O}_K$. Also $\gcd(d, d') \mid (d - d')$. Therefore we get

$$\gcd(d, d') \left| \frac{d - d'}{s} \right. .$$

From this, we write

$$|N(\gcd(d, d'))| \text{ divides } \frac{|N(d - d')|}{|N(s)|}.$$

Therefore

$$|N(\gcd(d, d'))| \leq \frac{|N(d - d')|}{|N(s)|}.$$

So, by (2), we conclude that

$$|N(\gcd(d, d'))| \leq \frac{\alpha \max\{|N(d)|, |N(d')|\}}{|N(s)|} \leq \frac{\max\{|N(d)|, |N(d')|\}}{|N(n)|^{1/3}},$$

since $|N(s)| \geq \alpha |N(n)|^{1/3}$. From this, we obtain

$$(1/3)\log|N(n)| \leq \max\left\{\log\left(\frac{|N(d)|}{|N(\gcd(d, d'))|}\right), \log\left(\frac{|N(d')|}{|N(\gcd(d, d'))|}\right)\right\},$$

that is,

$$(1/3)w(V(n)) \leq \max\{w(V(d) - V(d')), w(V(d') - V(d))\},$$

since $V(\gcd(d, d')) = V(d) \cap V(d')$. This proves (iii).

4. Proof of Theorem 2

Let $\delta, \lambda \in G$ such that

$$\delta(\alpha) = \min\{\sigma(\alpha) : \sigma \in G\} \text{ and } \lambda(\beta) = \min\{\sigma(\beta) : \sigma \in G\}.$$

Without loss of generality, we can assume that $\lambda(\beta) \leq \delta(\alpha)$. Therefore, for any $\sigma \in G$, we have

$$\sigma(\beta) \leq \Delta\lambda(\beta) \leq \Delta\delta(\alpha) \leq \Delta\sigma(\alpha).$$

This implies that

$$|N(\alpha - \beta)| \leq \Delta^{|G|-1} \max\{N(\alpha), N(\beta)\},$$

since

$$|N(\alpha - \beta)| = \prod_{\sigma \in G} |(\sigma(\alpha) - \sigma(\beta))| \leq \prod_{\sigma \in G} \max\{\sigma(\alpha), \sigma(\beta)\}.$$

This proves the theorem.

5. Proof of Theorem 3

Choose $\alpha = \Delta^{|G|-1}$ in Theorem 1. Then we have that any collection $\mathcal{A} \subseteq \mathcal{O}_K$ such that d divides n; $d \equiv r \pmod{s}$;

$$|N(d - d')| \leq \Delta^{|G|-1} \max\{|N(d)|, |N(d')|\} \tag{3}$$

and if d is not an associate of d', then $|N(d)| \neq |N(d')|$ for all $d, d' \in \mathcal{A}$, has at most 11 elements. Now we shall choose $\mathcal{A}$ as the set of all elements $d \in \mathcal{O}_K$ satisfying conditions (1), (2), (3) and (4) of this theorem. Then, by Theorem 2, condition (4) implies (3). This proves the theorem.

Acknowledgement

The author would like to thank Prof. R Srikanth (SASTRA University) and Prof. R Thangadurai (Harish-Chandra Research Institute) for their constant guidance and encouragement. He would also like to thank the referee of this paper for his/her valuable suggestions.

References

[1] Lenstra H W, Divisors in residue classes, *Math. Comp.* **42(165)** (1984) 331–340
[2] Luca F and Togbe A, On the positive integral solutions of the diophantine equation $x^3 + by + 1 - xyz = 0$, *Bull. Malays Math. Sci. Soc.* **31(2)** (2008) 129–134
[3] Mohanty S P and Ramasamy A M S, On the positive integral solutions of the Diophantine equation $x^3 + by + 1 - xyz = 0$ $(b > 0)$, *Bull. Malaysian Math. Soc.* **7(1)** (1984) 23–28
[4] Subburam S, On the positive integral solutions of the diophantine equation $x^3 + by + 1 - xyz = 0$, *Ramanujan J.* **32(2)** (2013) 203–219
[5] Wikstrőm D, On the l-ary GCD-algorithm in rings of integers, Lecture Notes in Comput. Sci., 3580 (2005) (Berlin: Springer) pp. 1189–1201