

Remarks on P-orderings and simultaneous orderings (Preprint)

István Járási
University of Debrecen

1 Preliminary definitions

Definition 1 (*S-Lenstra constant*) Let K be a number field, and \mathbb{Z}_K its ring of integers. Let S be a finite set of valuations of K containing all the infinite valuations. Let L be a maximal subset of \mathbb{Z}_K such that

$$x, y \in L \Rightarrow x - y \in \mathbb{Z}_{K,S}^*$$

where $\mathbb{Z}_{K,S}^*$ is the set of S -units in \mathbb{Z}_K . Then $\lambda_S(K) = \#L$ is called the S -Lenstra constant of K .

Remark 1 It is easy to see that the condition

$$x, y \in L \Rightarrow x - y \in \mathbb{Z}_{K,S}^*$$

is equivalent to

$$\prod_{0 \leq i < j \leq k} (a_i - a_j) \in \mathbb{Z}_{K,S}^*$$

if $L = \{a_0, a_1, \dots, a_k\}$. In fact we will use this second form of the condition.

Remark 2 We can assume that if L is such a maximal set, then $0, 1 \in L$. If $L = \{a_0, a_1, \dots, a_k\}$ then this can be achieved substituting a_i by $\frac{a_i - a_0}{a_1 - a_0}$.

What I have seen is only the definition of the S_∞ -Lenstra constant or simply the Lenstra constant of K (first in [11]).

The Lenstra constant was investigated several times, see [9], [5], [6], [7], [8], [12], [10], [11]. It is related to the norm-euclidicity of \mathbb{Z}_K .

To state our result we will need some more notation.

Definition 2 *Let m be a positive number. Let $S(m)$ denote the set of all valuations of K such that the corresponding primes has norm at most m , including the set S_∞ of the infinite valuations.*

Definition 3 *Let S be a set of valuations of K . Denote by $t_S(K)$ the smallest norm of the primes corresponding to valuations outside S .*

It is easy to see that we have

$$\lambda_S(K) \leq t_S(K)$$

for all S since the box principle: if one has more than $t_S(K)$ elements from \mathbb{Z}_K then there are two lying in the same residue class modulo a prime ideal having norm $t_S(K)$.

Definition 4 *Let P be a prime ideal of \mathbb{Z}_K . For all $a \in \mathbb{Z}_K$ let $w_P(a)$ denote the highest power of P that divides a .*

An infinite sequence $\{a_i\}_{i=0}^\infty$ of elements from \mathbb{Z}_K is called a P -ordering for P if for all $k \geq 1$ the element a_k is chosen such that

$$w_P((a_k - a_0)(a_k - a_1) \dots (a_k - a_{k-1})) \text{ is minimal.}$$

An infinite sequence $\{a_i\}_{i=0}^\infty$ (shortly $\{a_i\}$) of elements from \mathbb{Z}_K is called a simultaneous ordering if it is a P -ordering for all primes in \mathbb{Z}_K .

If we have a simultaneous ordering in \mathbb{Z}_K , then it is easy to compute the factorials:

Theorem 1 *(Bhargava [2]) If $\{a_i\}$ is a simultaneous ordering, for fixed k we have*

$$k!_{\mathbb{Z}_K} = \prod_{i=0}^{k-1} (a_k - a_i).$$

But there is another way to compute the factorials:

Theorem 2 (Bhargava [2]) For every k we have

$$k!_{\mathbb{Z}_K} = \prod_P w_P(k!_{\mathbb{Z}_K})$$

where

$$w_P(k!_{\mathbb{Z}_K}) = P^{\sum_{j=1}^{\infty} \left\lfloor \frac{k}{N(P)^j} \right\rfloor}.$$

2 Simultaneous orderings and S-Lenstra constants

Our result is the following

Theorem 3 To have a simultaneous ordering $\{a_i\}$ in \mathbb{Z}_K , it is necessary to have

$$\lambda_{S(m)}(K) = t_{S(m)}(K)$$

for every m .

PROOF: Let m be fixed. Since $\{a_i\}$ is a simultaneous ordering, for any k we have

$$k!_{\mathbb{Z}_K} = \prod_{i=0}^{k-1} (a_k - a_i).$$

This means that we have

$$\prod_{0 \leq i < j \leq k} (a_i - a_j) = \prod_{i=0}^k i!_{\mathbb{Z}_K}.$$

Since we also have

$$w_P(k!_{\mathbb{Z}_K}) = P^{\sum_{j=1}^{\infty} \left\lfloor \frac{k}{N(P)^j} \right\rfloor}$$

this concludes that the first prime outside $S(m)$ must appear in $(t_{S(m)})!_{\mathbb{Z}_K}$. So for $\{a_0, a_1, \dots, a_{t_{S(m)}-1}\}$ we have that

$$\prod_{0 \leq i < j \leq t_{S(m)}-1} (a_i - a_j) = \prod_{l=0}^{t_{S(m)}-1} l!_{\mathbb{Z}_K}$$

and this is divisible only by primes in $S(m)$, hence

$$t_{S(m)} = \#\{a_0, a_1, \dots, a_{t_{S(m)}-1}\} \leq \lambda_{S(m)}(K)$$

which with our previous remark shows that

$$\lambda_{S(m)}(K) = t_{S(m)}(K)$$

and $\{a_0, a_1, \dots, a_{t_{S(m)}-1}\}$ is a good sample to illustrate it.

In fact the following stronger theorem should also holds:

Theorem 4 *To have a simultaneous ordering $\{a_i\}$ in \mathbb{Z}_K , it is necessary to have*

$$\lambda_S(K) = t_S(K)$$

for every S containing S_∞ .

I do not provide the proof here.

Note that it is a necessary, but not sufficient condition, since for the set that gives the S-Lenstra constant we require only that the differences should be S-units, but not minimizing the maximal power of the prime ideal from S dividing the difference.

Theorem 3 has the following consequence:

Corollary 1 *Let $d \neq -3, 5$ be a squarefree integer such that $d \equiv 5 \pmod{8}$ and let $K = \mathbb{Q}(\sqrt{d})$. Then there is no simultaneous ordering in \mathbb{Z}_K .*

To prove this theorem we need the following definition and proposition.

Definition 5 *Let S be a finite set of valuations of K containing S_∞ . An element $a \in \mathbb{Z}_{K,S}$ is called an exceptional S-unit if*

$$a(1-a) \in \mathbb{Z}_{K,S}^*$$

The exceptional S_∞ -units are simply called exceptional units.

Proposition 1 *(Leutbecher-Martinet [5]) There are only 8 exceptional units of degree 2.*

PROOF: Let ε be an exceptional unit of degree two. Then it is necessary to have $a, b \in \mathbb{Z}$ such that

$$\varepsilon^2 + a\varepsilon \pm 1 = 0 \quad \text{and} \quad (1-\varepsilon)^2 + b(1-\varepsilon) \pm 1 = 0.$$

Obviously the second condition is equivalent to

$$\varepsilon^2 + (-b - 2)\varepsilon + (b + 1 \pm 1) = 0.$$

Since the defining polynomial of ε is unitary we have

$$a = -b - 2 \quad \text{and} \quad \pm 1 = b + 1 \pm 1$$

where the \pm signs in the second equation are independent. This means that we have 4 possibilities for the pairs (a, b) . One can check that all the four pairs corresponds to an exceptional unit ε . Since if ε is an exceptional unit, then $1 - \varepsilon$ is also an exceptional unit, the remaining 4 exceptional unit of degree 2 can be constructed.

One can easily check that $\lambda(K) \geq 3$ is equivalent to have an exceptional unit in \mathbb{Z}_K . Using this and our proposition it is easy to see that $\lambda(K) \geq 3$ can be stated only for two quadratic fields: for $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{5})$. In any other quadratic field we have $\lambda(K) = 2$. In fact $\lambda(\mathbb{Q}(\sqrt{-3})) = 3$ and $\lambda(\mathbb{Q}(\sqrt{5})) = 4$.

Now we can prove our corollary.

PROOF: Use our theorem with S_∞ . Let $K = \mathbb{Q}(\sqrt{d})$ with d satisfying the conditions of the theorem. It is showed above that the Lenstra constant of K is $\lambda_{S_\infty}(K) = 2$. Since 2 is irreducible in O_K we have $N_{K/\mathbb{Q}}(2) = 4$, and since $N_{K/\mathbb{Q}}(3) \geq 3$ we have

$$t_{S_\infty}(K) \geq 3 > \lambda_{S_\infty}(K) = 2,$$

therefore there is no simultaneous ordering in \mathbb{Z}_K .

Concerning the results of Bhargava one can see that we can start a simultaneous ordering with any element. To make our life easier we should choose the first element to be 0. It is equivalent to decrease all the elements of the P-ordering with the first element. If a is the second element then $w_P(a - 0)$ must be minimal for all P . This holds when a is a unit of the number field. This unit can be $a = 1$, so we shall fix the second element also. It is equivalent to divide all the elements of the P-ordering with the second element. The procedure described above shows that it is enough to deal with these "normalized" simultaneous orderings.

Since we know the units of imaginary quadratic fields, we can show the following:

Theorem 5 *Let d be a squarefree negative integer such that $d \equiv 2$ or 3 or 6 or $7 \pmod{8}$ and let $K = \mathbb{Q}(\sqrt{d})$. Then there is no simultaneous ordering in \mathbb{Z}_K .*

PROOF: In such a \mathbb{Z}_K we have $2 = P_1^2$ for a prime ideal P_1 . It is also clear that

$$2!_{\mathbb{Z}_K} = \prod_P w_P(2!_{\mathbb{Z}_K})$$

where

$$w_P(2!_{\mathbb{Z}_K}) = P^{\sum_{j=1}^{\infty} \left\lfloor \frac{2}{N(P)^j} \right\rfloor}.$$

Hence we have

$$2!_{\mathbb{Z}_K} = P_1.$$

If we have a normalized simultaneous ordering, then for its third element (denote it by a_2) we have

$$2!_{\mathbb{Z}_K} = (1 - a_2)(0 - a_2) = a_2(a_2 - 1)$$

so we have to solve the equation

$$a_2(a_2 - 1) = P_1$$

in \mathbb{Z}_K . Since P_1 is a prime ideal a_2 or $a_2 - 1$ must be a unit. But we have only finitely many units, and one can check that none of them solves our equation.

Using the ideas of our last proof, one can see that in the remaining case i.e. when $d = 1 \pmod 8$ we have

$$2!_{\mathbb{Z}_K} = 2 = P_1 P_2.$$

Since $a_0 = 0$, $a_1 = 1$, and $a_2 = 2$ is a good choice to satisfy this equation in every number field.

3 P-orderings and the structure of the corresponding subset

In what follows R will be a Dedekind ring, $S \subset R$, P a prime ideal of R of finite norm and $\{a_0, \dots, a_k\}$ elements from S .

One can see that the exponent of P in $w_P(\prod_{i=0}^{k-1} (a_k - a_i))$ depends only on the number of elements of the set $\{a_0, \dots, a_{k-1}\}$ in the residue classes mod P^j which also contains a_k . It motivates the following definition:

Definition 6 Let S be an arbitrary subset of the ring of integers of a number field, a_0, \dots, a_{k-1} be given elements of S . Let P be a prime ideal of norm N and m_0, \dots, m_{N-1} a complete set of residues mod P . Choose $\pi \in P \setminus P^2$. Then for every $l \geq 1$ integers let

$$n_k(i_0, \dots, i_{l-1}) = \#((m_{i_0} + m_{i_1}\pi + \dots + m_{i_{l-1}}\pi^{l-1}) \cap \{a_0, \dots, a_{k-1}\})$$

for every $(i_0, \dots, i_{l-1}) \in \{0, \dots, N-1\}^l$ where $(m_{i_0} + m_{i_1}\pi + \dots + m_{i_{l-1}}\pi^{l-1})$ stands for the mod P^l residue class containing $m_{i_0} + m_{i_1}\pi + \dots + m_{i_{l-1}}\pi^{l-1}$.

It is easy to see that the following equations hold:

$$\sum_{i_0=0}^{N-1} \dots \sum_{i_{l-1}=0}^{N-1} n_k(i_0, \dots, i_{l-1}) = k$$

and

$$\sum_{i=0}^{N-1} n_k(i_0, \dots, i_{l-2}, i) = n_k(i_0, \dots, i_{l-2}). \quad (1)$$

Using this definition it is easy to determine $w_P(\prod_{i=0}^{k-1}(a - a_i))$ for every $a \in S$. We have the following

Lemma 1 We have

$$w_P\left(\prod_{i=0}^{k-1}(a - a_i)\right) = P^{\sum_{l=1}^{\infty} n_k(i_0, \dots, i_{l-1})}$$

where the i_j -s are determined by the following congruences:

$$a \equiv m_{i_0} + m_{i_1}\pi + \dots + m_{i_{l-1}}\pi^{l-1} \pmod{P^l} \quad (2)$$

for every $l \geq 1$.

PROOF: It is easy to see that when the sum $\sum_{l=1}^{\infty} n_k(i_0, \dots, i_{l-1})$ is finite, the equality holds.

To see the finiteness, note that this sum contains all $n_k(i_0, \dots, i_{l-1})$ for $l \geq 1$ of the residue classes which contains also a . The series of the $n_k(i_0, \dots, i_{l-1})$ corresponding to the congruence condition 2 are monoton decreasing as l increases since (1). Let

$$n_{k+1}(i_0, \dots, i_{l-1}) = \#((m_{i_0} + m_{i_1}\pi + \dots + m_{i_{l-1}}\pi^{l-1}) \cap \{a_0, \dots, a_{k-1}, a\}).$$

Then we have

$$n_k(i_0, \dots, i_{l-1}) \leq n_{k+1}(i_0, \dots, i_{l-1}).$$

But the series of $n_{k+1}(i_0, \dots, i_{l-1})$ is also decreasing, and will be constant 1 after finitely many steps. Clearly this one element will be a , so the corresponding $n_k(i_0, \dots, i_{l-1})$ will be 0.

The definition of the $n_{k+1}(i_0, \dots, i_{l-1})$ implies that there exists an l such that all the elements of $\{a_0, \dots, a_{k-1}, a\}$ lies in different residue classes mod P^l . Therefore the series of $n_{k+1}(i_0, \dots, i_{l-1})$ corresponding to 2 will be constant 1 after finitely many steps.

Now it is clear that to choose the $k+1$ -st element $a = a_k$ of a P-ordering is equivalent to choose an element a with minimal $\sum_{l=1}^{\infty} n_k(i_0, \dots, i_{l-1})$. When $S = R$ this minimum is $\sum_{l=1}^{\infty} \lfloor \frac{k}{N^l} \rfloor$. It is true in more general situations also:

Theorem 6 *Let $S \subset R$ such that $R \setminus S$ is finite or assume that for every $l \geq 1$ every residue class mod P^l contains infinitely many elements of S . Then*

$$w_P(k!_S) = w_P(k!_R)$$

for every $k \geq 0$.

PROOF: To see this, note that $\sum_{l=1}^{\infty} n_k(i_0, \dots, i_{l-1})$ is the sum of the number of the set $\{a_0, \dots, a_{k-1}\}$ in the residue classes, so we have to choose only an appropriate residue class, and from this class any element is suitable.

This theorem has the following corollary:

Corollary 2 *Let $S \subset R$ such that $R \setminus S$ is finite. Then*

$$k!_S = k!_R$$

for every $k \geq 0$.

In what follows we formulate a conjecture stating that a P-ordering of S measures the distribution of S among the residue classes mod P^j . For simplicity we assume that P has finite norm.

In [9] Bhargava gives a P-ordering. This is the following:

Example 1 Let N be the norm of P and m_0, \dots, m_{N-1} a complete set of residues mod P . Choose $\pi \in P \setminus P^2$. For $i > 0$, write

$$i = c_0 + c_1N + \dots + c_hN^h$$

with $0 \leq c_j < N$, and define

$$a_i = m_{c_0} + m_{c_1}\pi + \dots + m_{c_h}\pi^h.$$

Then $\{a_i\}$ is a P -ordering, and

$$w_P\left(\prod_{i=0}^{k-1} (a_k - a_i)\right) = P^{\sum_{j \geq 1} \lfloor \frac{k}{N^j} \rfloor}.$$

Note that for given $l > 1$ in the residue class of $a_{i_0} + a_{i_1}\pi + \dots + a_{i_{l-1}}\pi^{l-1}$ there are $\lfloor \frac{k}{N^l} \rfloor$ or $\lfloor \frac{k}{N^l} \rfloor + 1$ elements of $\{a_0, \dots, a_k\}$. Equivalently: the elements of the P -ordering are uniformly distributed among the residue classes mod P^l .

My conjecture is that it is also the case when S is a proper subset of R .

Conjecture 1 If $\{a_i\}$ is P -ordering in $S \subset R$, then for every $k \geq 1$ and $l \geq 1$ the first k elements of $\{a_i\}$ are uniformly distributed on the intersections of the residue classes mod P^l and S .

This conjecture would imply the following:

Conjecture 2 Let S_1 and S_2 be two subsets of R such that there is an $l \geq 1$ and a residue class mod P^l such that the intersection of this class with S_1 and S_2 has different number of elements. Then there is an $k \geq 1$ such that

$$k!_S \neq k!_R.$$

In fact it is true that for every k there is a minimal l such that every residue class mod P^l contains at most 1 element of the first $k - 1$ element of the fixed P -ordering. It can be proved in an indirect way.

Clearly there must be a minimal $l' \geq l$ with the same property and with the additional property that there is a residue class C modulo $P^{l'}$ that does not contain any of the first $k - 1$ element of the P -ordering, but contains at least one element of S .

To choose the k -th element (assuming my conjecture) we have to choose one element of S from C . When P has finite norm, this can be done.

There is another corollary of the first conjecture. To formulate it, we define the P -tree of S as follows. Since for every $l > 0$ any residue class modulo P^l can be covered by $N(P)$ residue classes modulo P^{l+1} , all the residue classes modulo all possible P^l can be represented as a tree which has the residue classes as vertices, and two vertices are connected by an edge if one contains the other. Then it is obvious that all vertices has equal rank $N(P)$. Let write at each vertices the number of elements of the intersection of the the corresponding residue class and S . It is called the P -tree of S . Then, assuming the conjecture, we have

Conjecture 3 *Let S_1 and S_2 are subsets of R with the same P -tree. Then for all $k \geq 0$ one has*

$$w_P(k!_{S_1}) = w_P(k!_{S_2})$$

and conversely.

These are the first conjectures on the Question of the research plan [4]. It is expected that this will lead at least to partial answers on the Question 27 and 28 of Bhargava [2] (these are Question 1 and 2 in the research plan [4]).

References

- [1] Bhargava, Manjul *P-orderings and polynomial functions on arbitrary subsets of Dedekind rings*. J. reine angew. Math. **490** (1997), 101–127
- [2] Bhargava, Manjul *The Factorial Function and Generalizations*. Amer. Math. Monthly, **107** (2000), 783–799
- [3] Györy, K. *On a problem of A. M. Odlyzko on algebraic units of bounded degree*. Acta Math. Hungar. 69 (1995), no. 1-2, 1–4
- [4] Járási, I. *Research Report and Research Plan*
- [5] Leutbecher, Armin; Martinet, Jacques *Lenstra’s constant and Euclidean number fields*. Arithmetic Conference (Metz, 1981), 87–131, Astérisque, 94, Soc. Math. France, Paris, 1982

- [6] Leutbecher, Armin *Euclidean fields having a large Lenstra constant*. Ann. Inst. Fourier (Grenoble) 35 (1985), no. 2, 83–106
- [7] Leutbecher, Armin; Niklasch, Gerhard *On cliques of exceptional units and Lenstra’s construction of Euclidean fields*. Number theory (Ulm, 1987), 150–178, Lecture Notes in Math., 1380
- [8] Lenstra, H. W., Jr. *Euclidean number fields of large degree*. Invent. Math. 38 (1976/77), no. 3, 237–254
- [9] Martinet, Jacques *Sur la constante de Lenstra des corps de nombres*. Seminar on Number Theory, 1979–1980 (French), Exp. No. 17, 21 pp., Univ. Bordeaux I, Talence, 1980
- [10] Mestre, Jean-François *Corps euclidiens, unités exceptionnelles et courbes elliptiques*. J. Number Theory 13 (1981), no. 2, 123–137
- [11] Martinet, Jacques *Sur la constante de Lenstra des corps de nombres*. Seminar on Number Theory, 1979–1980 , Exp. No. 17
- [12] Queme, Roland *A computer algorithm for finding new Euclidean number fields*. J. Théor. Nombres Bordeaux 10 (1998), no. 1, 33–48
- [13] Wood, Melanie *P-orderings: a metric viewpoint and the non-existence of simultaneous orderings*. J. Number Theory, **99** (2003) 36–56.