Computer Science Journal of Moldova, vol.**29**, no.2(86), 2021

Cube-root-subgroups of SL_2 over imaginary quadratic integers*

Miroslav Kureš

Abstract

All cube roots of the identity in the special linear group of 2×2-matrices with entries in the ring of integers in $\mathbb{Q}[\sqrt{d}]$ are described. These matrices generate subgroups of the third order; it is shown that such subgroups may contain non-elementary matrices in the sense of P. M. Cohn. All this is viewed with respect to possible applications in lattice cryptography.

Keywords: Imaginary quadratic field, ring of integers, non-elementary matrices, special linear group, public-key cryptography, lattice-based cryptosystems.

MSC 2010: 13F07, 15A16, 11R11, 11T71.

1 Introduction

Some public-key cryptographic algorithms are believed to be secure against attacks by quantum computers. Lattice-based cryptography is believed to be one of them ([1]). Another system is e. g. multivariate public key cryptography (we discuss some of its features and possible improvements in the papers [3] and [4], where the multivariate system is called TTM, which means the Tame Transformation Method).

On the other hand, Shor's algorithm for quantum computers is designed to solve prime factorization of large primes and the discrete logarithm problem in polynomial time.

In the paper, we will have in mind – in the background – lattices represented by their generator matrices. We are concerned with design

*The research has been supported by Brno University of Technology, the specific research plan No. FSI-S-20-6187.

ideas based on linear algebra over certain domains. Regarding the submission of these ideas into a lattice-based cryptosystem, we can think, for instance, the GGH cryptosystem, which is perhaps the most intuitive encryption scheme based on lattices. We remark that the classical GGH cryptosystem has been subject to cryptanalytic attacks and should be considered insecure, but we are not particularly limited to this system, which we mention as an example only, and, moreover, we present a completely different algebraic situation in which no attacks have yet been proposed.

In some cryptographic protocols working over finite groups, we have to be careful that we do not fall victim to what is called a *small subgroup attack*. In order to counter this attack, the prime order groups are used, in which all elements are primitive and small subgroups do not exist ([8]).

So, our design is to consider lattice cryptography over imaginary quadratic integers, involving not only large-size matrices but also 2×2 matrices, then selecting non-elementary matrices that are difficult to generate. In this paper we note that there exist also inappropriate, small subgroups in this case. Our result can also be seen as a contribution to matrix theory.

2 Some facts about orders of imaginary quadratic fields and problem formulation

Let d be a negative square-free integer and C a positive integer. We will distinguish two cases:

(I) $d \equiv 1 \pmod 4$

(II) $d \equiv 2$ or $d \equiv 3 \pmod 4$

We set

$$\varepsilon = \begin{cases} 1 & \text{for the case (I)} \\ 0 & \text{for the case (II);} \end{cases}$$

and

$$\theta = \sqrt{d} + \frac{\varepsilon}{2}\left(1 - \sqrt{d}\right)$$

and

$$D = -d + \frac{\varepsilon}{4}(1 + 3d).$$

Further, we denote by $\mathbb{Z}[C\theta]$ an *order of the imaginary quadratic field* $\mathbb{Q}[\sqrt{d}]$, so

$$\mathbb{Z}[C\theta] = \{x + yC\theta; x, y \in \mathbb{Z}\}.$$

The order $\mathbb{Z}[C\theta]$ is a normed ring with the norm $|\ |\colon \mathbb{Z}[C\theta] \to \mathbb{R}^+$ equal to the complex numbers absolute value. Then for $z = x + yC\theta \in \mathbb{Z}[C\theta]$ we have

$$|z|^2 = x^2 + \varepsilon xyC + y^2C^2D.$$

All orders are domains. For $C = 1$, the order $\mathbb{Z}[C\theta]$ is called the *maximal order* or the *ring of integers* in $\mathbb{Q}[\sqrt{d}]$ (often denoted also by $\mathcal{O}_{Q[\sqrt{d}}$).

The maximal orders are principal ideal domains (PID's) if and only if d is one of the numbers

$$-1, -2, -3, -7, -11, -19, -43, -67, -163.$$

For the (more usual) norm defined as the square root of our $|\ |$, there does not exist any $x \in \mathbb{Z}[\theta]$ with this norm between 1 and 2 (or in our $|\ |$ between 1 and 4) which holds for every negative square-free d, excerpt when

$$d = -1, -2, -3, -7, -11$$

which are just the domains in which is a Euclidean algorithm for computing the greatest common divisor. All other $\mathbb{Z}[\theta]$ are non-Euclidean.

2.1 The fact that not all matrices are elementary

Let us consider $\mathrm{SL}(2, \mathbb{Z})$. By an *elementary transvection* $V_{ij}(r)$ $1 \leq i \neq j \leq m$, $r \in R$, we mean a matrix $[a_{\nu\mu}]$ with

$$a_{\nu\mu} = \begin{cases} 1_R & \text{for } \nu = \mu \\ r & \text{for } \nu = i, \mu = j \\ 0_R & \text{otherwise.} \end{cases}$$

Finite products of elementary transvections form a subgroup $\mathrm{SE}(2,\mathbb{Z})$ of *elementary matrices* in $\mathrm{SL}(2,\mathbb{Z})$. In other words, one can obtain elementary matrices by a finite sequence of multiplyings a row (or column) by a non-zero number r and adding the result to another row (or column), starting from the identity matrix. However, $\mathrm{SE}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z})$.

When we replace $\mathbb{Z}$ by another ring R, then it can happen that $\mathrm{SE}(2,R)$ is a proper subgroup of $\mathrm{SL}(2,R)$. This problem was studied by P. M. Cohn in 1966. He was the first to give an example of a matrix with determinant 1 which is not elementary. In the paper [5] (published in 2011), we introduced an algorithm how to detect such matrices for any order of imaginary quadratic field.

2.2 Some classical examples of non-elementary matrices

Here are some known examples of non-elementary matrices that have been studied before. By way of illustration, we also calculate their twelfth power: these matrices are of infinite order, so the norms of their entries are not bounded.

P. M. Cohn, [2], 1966: $d = -19$,

$$M_{\mathsf{Cohn}} = \begin{pmatrix} 3-\theta & 2+\theta \\ -3-2\,\theta & 5-2\,\theta \end{pmatrix}.$$

Then

$$M_{\mathsf{Cohn}}^{12} = \begin{pmatrix} -138533292392+7105318818\,\theta & 1003585011-60934202901\,\theta \\ -29430829974+110698224819\,\theta & -249231517211+23358797787\,\theta \end{pmatrix}.$$

R. Tuler, [9], 1983: $d = -37$,

$$M_{\mathsf{Tuler}} = \begin{pmatrix} 29 & 7-\theta \\ 7+\theta & 3 \end{pmatrix}.$$

We compute

$$M_{\mathsf{Tuler}}^{12} = \begin{pmatrix} 1033551428421627457 & 249747318595287744-35678188370755392\,\theta \\ 249747318595287744+35678188370755392\,\theta & 105918530781987265 \end{pmatrix}.$$

This paper shows that there are also small-order non-elementary matrices for which even the third power is the identity matrix. For example, for $d = -163$ all matrices

$$M_1 = \begin{pmatrix} 1 - 5\,\theta & 2 + 2\,\theta \\ 19 - 12\,\theta & -2 + 5\,\theta \end{pmatrix},$$

$$M_2 = \begin{pmatrix} 4 - \theta & 5 + 2\,\theta \\ 4 & -5 + \theta \end{pmatrix},$$

$$M_3 = \begin{pmatrix} 8 - \theta & 4 - 2\,\theta \\ -8 & -9 + \theta \end{pmatrix},$$

and

$$M_4 = \begin{pmatrix} -10 - 3\,\theta & 25 + 4\,\theta \\ -2 - 2\,\theta & 9 + 3\,\theta \end{pmatrix}$$

are examples of non-elementary matrices, the third power of which is I.

Theorem 2.7 of [6] allows us to calculate easily the possible orders of elements of $\mathrm{GL}\,(2, \mathbb{Z})$. The result is that this group can have subgroups of orders 2, 3, 4, and 6. We note that all these numbers are divisors of 12, whose power we have calculated above. [1]

2.3 The problem

We search for matrices M whose entries are integers in $\mathbb{Q}[\sqrt{d}]$ satisfying

$$M^3 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

[1] When we have already mentioned divisors of the number 12, we will also remember the efforts of the duodecimalists, by recalling Limerick from the Duodecimal Bulletin 2015, No.1:
A base boasting reason and rhyme,
Sported factors full four at a time.
"Why the fourth and the third?"
"Cause just three is absurd;
And only two, sir, is a crime."

Our next requirement is that the determinant of the matrix M is equal to 1. So, we do not consider matrices like $\begin{pmatrix} 1 & 0 \\ 0 & \frac{-1+\sqrt{-3}}{2} \end{pmatrix}$; in other words, we are only in the group $\mathrm{SL}\,(2, \mathbb{Z}\,[\theta])$.

Of course, trivial solutions of the problem $M^3 = I$ are diagonal matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} \frac{-1+\sqrt{-3}}{2} & 0 \\ 0 & \frac{-1+\sqrt{-3}}{2} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \frac{-1-\sqrt{-3}}{2} & 0 \\ 0 & \frac{-1-\sqrt{-3}}{2} \end{pmatrix},$$

the last two only in the case of Eisenstein integers. We want to classify all other nontrivial matrices.

3 The result

Theorem 1. *Let d be a negative square-free integer. Then the complete classification of matrices of $\mathrm{SL}\,(2, \mathbb{Z}\,[\theta])$ representing nontrivial cube roots of identity is as follows.*

(i) For every $d \neq -3$, a matrix of $\mathrm{SL}\,(2, \mathbb{Z}\,[\theta])$ represents nontrivial cube roots of identity if and only if it is of a form

$$\begin{pmatrix} a + A\,\theta & b + B\,\theta \\ c + C\,\theta & -a - 1 - A\,\theta \end{pmatrix}, \tag{1}$$

where

$$bc + BC\left(d - \varepsilon\frac{3d+1}{4}\right) = -1 - a - a^2 - A^2\left(d - \varepsilon\frac{3d+1}{4}\right) \tag{2}$$

$$bC + Bc + \varepsilon BC = -A - 2aA - A^2, \tag{3}$$

$a, A, b, B, c, C \in \mathbb{Z}$.

(ii) For $d = -3$, a matrix of $\mathrm{SL}\,(2, \mathbb{Z}\,[\theta])$ is of the same form as in the case (i).

(iii) The cardinality of the intersection of a 3-element subgroup generated by a nontrivial cube root of identity with $\mathrm{SE}\,(2, \mathbb{Z}\,[\theta])$ can be either 1 or 3.

Proof. (i) Let us start with a matrix

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{C}$. One can easily deduce that requirement $M^3 = I$ implies the following system of equations:

$$\begin{aligned} \alpha^3 + 2\alpha\beta\gamma + \beta\gamma\delta &= 1; && (4)\\ \beta\left(\alpha^2 + \beta\gamma + \alpha\delta + \delta^2\right) &= 0; && (5)\\ \gamma\left(\alpha^2 + \beta\gamma + \alpha\delta + \delta^2\right) &= 0; && (6)\\ \alpha\beta\gamma + 2\beta\gamma\delta + \delta^3 &= 1. && (7) \end{aligned}$$

Equations (5) and (6) are directed to three variants.

Variant I. Let $\beta = 0$. Then $\alpha^3 = 1$ and $\delta^3 = 1$. Let us denote by $\sigma = \frac{-1+\sqrt{3}}{2}$ and by $\bar{\sigma}$ its complex conjugate. Then the set of complex cube roots of 1 is $S = \{1, \sigma, \bar{\sigma}\}$. Then $\alpha = \sigma_1$, $\delta = \sigma_2$, where σ_1 and σ_2 are some elements from S. Now, it follows from the equation (6) that if $\sigma_1 = \sigma_2$, then $\gamma = 0$, and if $\sigma_1 \neq \sigma_2$, then γ can be taken completely arbitrarily. The conclusion of this variant is therefore

$$\begin{pmatrix} \sigma_1 & 0 \\ \gamma & \sigma_2 \end{pmatrix} \qquad \text{with } \sigma_1,\ \sigma_2,\ \gamma \text{ as mentioned.} \qquad (8)$$

Variant II. Let $\gamma = 0$. Analogous to the previous Variant I. The conclusion is

$$\begin{pmatrix} \sigma_1 & \beta \\ 0 & \sigma_2 \end{pmatrix} \qquad \text{with } \sigma_1,\ \sigma_2,\ \beta \text{ similarly as above.} \qquad (9)$$

Variant III. Let $\beta \neq 0 \wedge \gamma \neq 0$. Then

$$\beta\gamma = -\alpha^2 - \alpha\delta - \delta^2.$$

If we substitute this into (4) or (7), we obtain equally

$$(\alpha + \delta)^3 = -1. \qquad (10)$$

Let $\widehat{S} = \{-1, -\sigma, -\bar{\sigma}\}$ and let $\widehat{\sigma}_0$ be an element from $\widehat{S}$ and $\bar{\widehat{\sigma}}_0$ its complex conjugate. Then

$$\beta\gamma = -\alpha^2 - \widehat{\sigma}_0 + \bar{\widehat{\sigma}}_0. \tag{11}$$

In conclusion, we have

$$\begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha + \widehat{\sigma}_0 \end{pmatrix}, \qquad \text{where } \widehat{\sigma}_0, \beta \text{ and } \gamma \text{ satisfy what has been just described.}$$

Non-Eisenstein integers ($d \neq -3$) do not contain elements σ, $-\sigma$, $\bar{\sigma}$ and $-\bar{\sigma}$. This brings a much simpler situation. In the *Variant I* as in the *Variant II*, we obtain only the identity matrix I. The *Variant III* reads as

$$\begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha - 1 \end{pmatrix}, \qquad \text{where } \beta\gamma = -\alpha^2 - \alpha - 1.$$

For a precise description of the condition $\beta\gamma = -\alpha^2 - \alpha - 1$, we write down complex numbers into components:

$$\alpha = a + A\theta, \;\; \beta = b + B\theta, \;\; \gamma = c + C\theta.$$

We derive from $\theta = \sqrt{d} + \frac{\varepsilon}{2}\left(1 - \sqrt{d}\right)$ that $\theta^2 = d + \varepsilon\left(\theta - \frac{3d+1}{4}\right)$ and compute directly (2) and (3).

We remark that for given $a, A \in \mathbb{Z}$, we can denote $A_1 = -1 - a - a^2 - A^2\left(d - \varepsilon\frac{3d+1}{4}\right)$, $A_2 = -A - 2aA - A^2$ (the right hand sides of (2) and (3)) and observe that there are many integer solutions for b, B, c and C, for example, $b = A_1$, $B = A_2$, $c = 1$, $C = 0$.

(ii) For $d = -3$, $\theta = \sqrt{-3} + \frac{1}{2}\left(1 - \sqrt{-3}\right) = \frac{1+\sqrt{-3}}{2}$. Then

$$S = \left\{1, -\theta, -\bar{\theta}\right\} \quad \text{and} \quad \widehat{S} = \left\{-1, \theta, \bar{\theta}\right\}.$$

The *Variant I* and *Variant II*, namely (8) and (9), lead to three trivial solutions, I, $\begin{pmatrix} -\theta & 0 \\ 0 & -\theta \end{pmatrix}$ and $\begin{pmatrix} -\bar{\theta} & 0 \\ 0 & -\bar{\theta} \end{pmatrix}$ and for solutions described in the special case.

In the *Variant III*, we have to add to equations (10) and (11) the additional equation, the requirement that the determinant of M is equal to 1. However,

$$\det M = \alpha\delta - \beta\gamma = \alpha\left(\widehat{\sigma}_0 - \alpha\right) - \left(-\alpha^2 + \alpha\widehat{\sigma}_0 + \bar{\widehat{\sigma}}_0\right) = -\bar{\widehat{\sigma}}_0.$$

Nevertheless, $-\bar{\widehat{\sigma}}_0 = 1$ means that $\bar{\widehat{\sigma}}_0 = -1$ and $\widehat{\sigma}_0 = -1$. Therefore, we have no equations other than those already derived in (iA).

(iii) We have a group with 3 elements

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha - 1 \end{pmatrix}, \quad M^2 = M^{-1} = \begin{pmatrix} -\alpha - 1 & -\beta \\ -\gamma & \alpha \end{pmatrix},$$
$$M^3 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

with $\beta\gamma = -\alpha^2 - \alpha - 1$. Of course, M^3 is elementary and M is elementary if and only if M^2 is elementary as elementary matrices form the group $\mathrm{SE}\left(2, \mathbb{Z}\left[\theta\right]\right)$. It remains to show that M can be both elementary and non-elementary. This can be demonstrated already for $d = -5$. Suitable matrices are, for example,

$$M_{\mathcal{E}} = \begin{pmatrix} 1 + \sqrt{-5} & -2 + 3\sqrt{-5} \\ -1 & -2 - \sqrt{-5} \end{pmatrix}$$

which is elementary and

$$M_{\mathcal{N}} = \begin{pmatrix} 2 - 7\sqrt{-5} & 1 + 2\sqrt{-5} \\ 28 - 21\sqrt{-5} & -3 + 7\sqrt{-5} \end{pmatrix}$$

which is non-elementary.

We present elementary transvections as elementary row opera-

tions. We observe

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \xrightarrow{\mathrm{r}_1=\mathrm{r}_1+\left(3+\sqrt{-5}\right)\mathrm{r}_2} \begin{pmatrix} 1 & 3+\sqrt{-5} \\ 0 & 1 \end{pmatrix}$$
$$\xrightarrow{\mathrm{r}_2=\mathrm{r}_2-\mathrm{r}_1} \begin{pmatrix} 1 & 3+\sqrt{-5} \\ -1 & -2-\sqrt{-5} \end{pmatrix}$$
$$\xrightarrow{\mathrm{r}_1=\mathrm{r}_1-\sqrt{-5}\mathrm{r}_2} \begin{pmatrix} 1+\sqrt{-5} & -2+3\sqrt{-5} \\ -1 & -2-\sqrt{-5} \end{pmatrix} = M_{\mathcal{E}}.$$

and that is why the matrix $M_{\mathcal{E}}$ is elementary.

For the proof of the non-elementarity of $M_{\mathcal{N}}$, we use approach presented in [5]. The $(1,2)$-submatrix of $M_{\mathcal{N}}$ is

$$A = \begin{pmatrix} 2-7\sqrt{-5} & 1+2\sqrt{-5} \end{pmatrix},$$

and the reduction ellipse $\mathcal{E}_{\mathrm{red}}$ has the equation

$$x^2 + 5y^2 + \frac{136}{21}x + \frac{110}{21}y + \frac{76}{7} = 0$$

(for the procedure of the computation see [5]). We can verify (or observe on the Figure 1) that there are no interior lattice points of the reduction ellipse with integer coordinates. Hence there are no reduction elements for A, and therefore $M_{\mathcal{N}}$ is non-elementary.

□

Remark 1. It is easy to search for *square roots* from the identity. But there are no non-trivial solutions in $\mathrm{SL}\,(2,\mathbb{Z})$, which the reader can verify. Another problem would be to look for the *fourth roots*, where the same procedure as in our paper could be used.

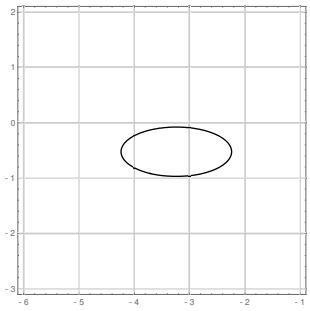

Figure 1. The reduction ellipse $\mathcal{E}_{\mathrm{red}}$ for the matrix A possessing no interior lattice point.

4 The Goldreich–Goldwasser–Halevi cryptosystem (GGH)

The private key is a generator matrix Z of a complete lattice $\mathcal{L}$ with good properties such as short and nearly orthogonal generators together with a unimodular matrix M.

The public key is another ("bad") generator matrix Y of $\mathcal{L}$ obtained as $Y = MZ$.

Given an open message expressed as a vector $\mathbf{m}$ and a random (so-called error) vector $\mathbf{e}$ which has to be small, we cipher by $\mathbf{c} = \mathbf{m} \cdot Y + \mathbf{e}$.

To decrypt $\mathbf{c}$, first compute $\mathbf{d} = \mathbf{c} \cdot Z^{-1}$ and apply the rounding-off which provides $\lfloor \mathbf{d} \rceil$. Finally, we compute $\mathbf{m}$ as $\lfloor \mathbf{d} \rceil \cdot M^{-1}$.

4.1 GGH cryptosystem – introductory example over Gaussian integers

Let $d = -1$, then $\theta = \sqrt{-1}$. We will present only a very basic example to remind the reader of the principles of the GGH system.

Let the generator matrix of the complete 3-lattice $\mathcal{L}$ be

$$Z = \begin{pmatrix} 12+\theta & 0 & 1+2\,\theta \\ 1 & 15+\theta & 1-\theta \\ 4-\theta & 3-3\,\theta & 11-19\,\theta \end{pmatrix},$$

and the unimodular matrix

$$M = \begin{pmatrix} 8+3\,\theta & -2+20\,\theta & 3+2\,\theta \\ 33-3\,\theta & 39+8\,\theta & 4-6\,\theta \\ 2+4\,\theta & 2+5\,\theta & 1 \end{pmatrix}$$

($\det M = 1$). Then the "bad" generator matrix of $\mathcal{L}$ is

$$Y = M \cdot Z = \begin{pmatrix} 105+69\,\theta & -35+295\,\theta & 91+6\,\theta \\ 448-23\,\theta & 571+129\,\theta & 16-110\,\theta \\ 26+54\,\theta & 28+74\,\theta & 12-8\,\theta \end{pmatrix}.$$

Now, for the open message $\mathbf{m} = (50+\theta, 11-\theta, 34+15\,\theta)$ and the error vector $\mathbf{e} = (1+\theta, 2-\theta, 3-2\,\theta)$, we compute the ciphered message as

$$\mathbf{c} = \mathbf{m} \cdot Y + \mathbf{e} = (10161+5081\,\theta, 4209+18498\,\theta, 5141-929\,\theta)\,.$$

The decryption: first, we compute $\mathbf{d} = \mathbf{c} \cdot Z^{-1}$ as

$$\left(\frac{2989188391}{3907301} + \frac{1008368124}{3907301}\theta, \frac{2423186121}{7814602} + \frac{4872178230}{3907301}\theta, \frac{860187474}{3907301} + \frac{375699873}{7814602}\theta\right)$$

which we round-off to

$$\lfloor \mathbf{d} \rceil = (765+258\,\theta, 310+1247\,\theta, 220+48\,\theta)\,.$$

Finally, $\mathbf{m}$ is recovered with

$$\mathbf{m} = \lfloor \mathbf{d} \rceil \cdot M^{-1} = (50+\theta, 11-\theta, 34+15\,\theta)\,.$$

4.2 GGH cryptosystem – a use of non-elementary matrices, where $d = -163$

For example, we can use a non-elementary unimodular matrix $M_{\mathcal{U}} = (M_1 \cdot M_2 \cdot M_3 \cdot M_4)^3$ as

$$\begin{pmatrix} 52573221941851385 + 7734170153866877\,\theta & -108339682589377105 - 8450168415298437\,\theta \\ 97004133663118053 + 22955204128735434\,\theta & -224828457848433395 - 29213244459035477\,\theta \end{pmatrix}.$$

We can use it for construction of a "bad" generator matrix. Then, a finding of the inverse matrix is complicated not only by that we have

used an "innovation" ring of integers with completely different multiplication compared to $\mathbb{Z}$ but also by the fact that MZ can also be non-elementary and attempting to break such an element of a cryptosystem precludes, for example, a use of Gauss-Jordan elimination for the inverse.

5 Conclusion

Computer science develops cryptographic protocols and judges how secure certain protocols are. The purpose of cryptography is to prevent other parties from accessing information they should not access. In our digitized world, these questions have considerable importance as communicating sides do not meet directly and use asymmetric cryptographic protocols. Modern public-key cryptography uses advanced algebraic methods. The paper deals with questions coinciding with the so-called small subgroup attack. There are classified all cube roots of the identity in the special linear group of second-order matrices with entries in the ring of integers in imaginary quadratic fields. The result may be essential for designing new protocols, e.g. in lattice-based cryptosystems.

Acknowledgements

The research has been supported by Brno University of Technology, the specific research plan being No. FSI-S-20-6187.

References

[1] *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Springer-Verlag Berlin Heidelberg, 2009, 256 p. DOI: 10.1007/978-3-540-88702-7. Hardcover ISBN: 978-3-540-88701-0.

[2] P. M. Cohn, "On the structure of GL_2 of a ring," *Publications Mathématiques de l'I.H.É.S.*, vol. 30, pp. 5–53, 1966. DOI: https://doi.org/10.1007/BF02684355.

[3] J. Hrdina, M. Kureš, and P. Vašík, "A note on tame polynomial automorphisms and the security of TTM cryptosystem," *Applied and Computational Mathematics*, vol. 9, no.2, pp. 226–233, 2010.

[4] M. Kureš, T. Decome, and G. Drecourt, "LoRi-TTM cryptosystem," *Annals of the University of Craiova, Mathematics and Computer Science Series*, vol. 45, no. 1, pp. 137–150, 2018.

[5] M. Kureš and L. Skula, "Reduction of matrices over orders of imaginary quadratic fields," *Linear Algebra and Its Applications*, vol. 435, no. 8, pp. 1903–1919, 2011.

[6] J. Kuzmanovich and A. Pavlichenkov, "Finite groups of matrices whose entries are integers," *The American Mathematical Monthly*, vol. 109, no. 2, pp. 173–186, 2002.

[7] B. Nica, "The unreasonable slightness of E_2 over imaginary quadratic rings," *The American Mathematical Monthly*, vol. 118, no. 5, pp. 455–462, 2011.

[8] C. Paar and J. Pelzl, *Understanding cryptography: a textbook for students and practitioners*, Springer, 2009, 390 p. ISBN: 978-3-642-04100-6. DOI: 10.1007/978-3-642-04101-3.

[9] R. Tuler, "Detecting products of elementary matrices in $GL_2(\mathbb{Z}[\sqrt{d}])$," *Proceedings of the American Mathematical Society*, vol. 89, no. 1, pp. 45–48, 1983.

Miroslav Kureš

Received May 3, 2021
Accepted July 18, 2021

Miroslav Kureš
Brno University of Technology
Technická 2, 61669 Brno, Czechia
Phone: +420 541142714
E–mail: kures@fme.vutbr.cz