ADVANCES IN CYBER-PHYSICAL SYSTEMS

Vol. 10, No. 2, 2025

HIGH ORDER UNITS IN GROUP RINGS SPECIFIED BY FINITE FIELD AND DIHEDRAL GROUP

Roksolana Oberyshyn, Roman Popovych

Lviv Polytechnic National University, 12, S. Bandery str., Lviv, 79013, Ukraine.
Authors' e-mails: *roksoliana.r.oberyshyn@lpnu.ua, roman.b.popovych@lpnu.ua*

https://doi.org/10.23939/acps2025.02.168

Submitted on 11.09.2025

***Abstract*: The basis of a significant amount of cryptographic systems for information protection are different computationally hard problems. One of these problems is finding the discrete logarithm value in a certain finite group. The problem is to obtain for any two given elements of this group such natural number that the first element to the power of the number equals the second element.**

In order to implement the cryptosystem, they have to choose an appropriate finite group and an element of high multiplicative order in it, so that computing the discrete logarithm is a hard problem. Powerful quantum computers will solve in polynomial time the discrete logarithm problem in the most common finite groups (multiplicative group of prime or extended finite field, group of points of elliptic curve over a finite field). That is why, as one of directions, they study groups consisting of invertible elements of group rings specified by various rings and groups. In the paper, the issue of finding high order units for special group rings, defined by finite field and dihedral group, is explored.

***Index terms*: discrete logarithm problem, group ring, finite field, dihedral group.**

I. INTRODUCTION

At the heart of most public key cryptosystems are the so called computationally hard problems. One such problem is obtaining the discrete logarithm in a suitably chosen finite group G: for given elements $g, h \in G$, find positive integer x such that $h = g^x$.

Based on this problem, Diffie and Hellman proposed protocol for two parties (Alice and Bob) to agree on a secret key using a public communication channel [1].

Alice chooses randomly a positive integer x and calculates the value g^x. Analogously, Bob chooses number y and calculates g^y. They exchange these elements and then count the same value (secret key) $K = (g^y)^x = (g^x)^y$. Slightly improving the considered construction, El-Gamal proposed an asymmetric cryptosystem.

The multiplicative order of element g is the smallest positive integer n with the condition $g^n = e$, where e is the group identity element. Both described cryptographic protocols give the correct result for an arbitrarily chosen element g. However, their resistance to hacking depends on how high is the element order.

To implement the mentioned cryptographic protocols, one must take a suitable finite group and high order element in it, that is to ensure that computing the discrete logarithm is a hard problem. The most well-known choices are the following: multiplicative group of prime finite field $F_p^* = \{1,2,...,p-1\}$, where p is a large prime (originally Diffie and Hellman used this group); multiplicative group of extended finite field; group of points of an elliptic curve over a finite field.

Quantum computers can solve efficiently the discrete logarithm problem in these three groups exploiting Shor algorithm [1]. This fact makes these constructions unreliable in the future. Because of this, research is being done that will ensure the resistance of cryptographic schemes in the coming era of quantum computers. One of such directions is using of algebraic structures called group rings [2].

Let ring with unity R and group G be given. Then the set of all possible records

$$R[G] = \{\sum_{i=0}^{t} r_i g_i \mid t = 0,1,2,...; r_i \in R, g_i \in G\}, \quad (1)$$

is called a group ring. Element u of the group ring is invertible (unit), if there exist element v of this ring, such that $uv=vu=1$ holds. The multiplicative group $U(R[G])$ of the ring consists of its units.

II. LITERATURE REVIEW AND PROBLEM STATEMENT

Group rings were not used in cryptography until the second decade of the 21st century. A public-key cryptosystem using group rings was first proposed in [3]. For encryption and decryption, units and the computational complexity of the discrete logarithm in group rings were used. Numerous applications of group rings in communications and digital signal processing are discussed in [4].

Two asymmetric cryptosystems based on group rings were suggested in [5]. The first one is an asymmetric cryptosystem over a group ring that combines elliptic curves and the El-Gamal construction, and the second one is an asymmetric cryptosystem over a group ring of the El-Gamal type without involving elliptic curves. Both

computational schemes use units of group rings. Two mentioned cryptosystems and generally group rings-based cryptosystems have a higher level of security than existing cryptosystems, since no quantum algorithm is currently known to solve efficiently (in polynomial time) the discrete logarithm problem in group rings [5]. In the coming era of quantum computers, this enhanced protection would play a significant role.

There is a significant number of publications on the structure of the unit group of a group ring. But only a few papers consider how to explicitly obtain elements of this group. However, the actual explicit construction of these elements, as well as ensuring that they have high order, is essential for using of group rings in cryptography.

Works [5, 6] describe how to search for units for a number of group rings. In particular, they use well-known environments for mathematical calculations GAP (LAGUNA, Wedderga packages), Magma, Matlab. Using the LAGUNA package of the GAP environment [5], the group of units of a group ring given by a finite field of p elements for some prime number p and a finite p-group can be efficiently computed for small values of p. However, as the number increases, the GAP environment becomes inefficient.

To define a group ring, different options for ring and group are considered. As ring they usually take finite field or ring of integers. Possible choices for group are as follows: finite cyclic group, dihedral group, permutation group. Research is also being conducted related to the use of LWE problem [7] or matrices over group rings [8, 9]. An issue of finding high order units in group rings given by finite field and finite cyclic group is investigated in [10]. Note that this group ring is commutative.

One of the promising directions is the study of the unit group of non-comutative group rings formed by a finite field and a finite dihedral group. Despite the availability of theoretical descriptions [11-13], explicitly finding such elements remains a difficult task, especially for large parameters. In [13] the structure of such rings is described under the condition that q is coprime with r and every prime divisor of the number r divides $q-1$. In [12] a review of works in which this condition is removed for some partial cases is made. Based on the literary survey, the unit group structure of group rings has been established for the following cases: $F_{2^n}[D_{2m}]$ (m is odd number), $F_{p^n}[D_{2p^m}]$ (p is odd prime), F_qD_{60}, F_qD_{40} and F_qD_{36}, where F_q denotes finite field with $q=p^n$ elements for some natural number n.

III. SCOPE OF WORK AND OBJECTIVES

The purpose of this work is to explore the potential of using Wedderburn-Artin theorem to describe the group of invertible elements (units) in one class of group rings. We consider such class of group rings, for which this theorem is applicable, and which are at the same time important for the implementation of cryptographic primitives that are resistant to different possible (pre-quantum and quantum) attacks.

This paper demonstrates how one can obtain a description of a group ring by considering a ring isomorphic to it.

The aim of this work is to investigate the problem of finding units in group rings formed by a finite field and a dihedral group. Of particular interest is the search for units of high order that can be used in cryptographic protocols such as Diffie-Hellman key exchange and ElGamal public key cryptosystem and ensure resistance to quantum attacks.

IV. OBTAINING ELEMENTS OF HIGH ORDER

We consider the case, when ring $R = F_q$ is a finite field, and group $G = D_r$ is a dihedral group (non-abelian for $r \geq 3$). This group describes the symmetries of regular r-gon and includes r rotations (in particular, the identity symmetry e) and r reflections. It is given by generators x and y, where x is the rotation by the angle $2\pi/r$, i.e. $x^r = e$, y is the reflection (mirror symmetry) such, that $y^2 = e$, and the additional relationship $yxy^{-1}=x^{-1}$. List of group elements is as follows:

$$D_r = \{1, x, x^2, \ldots, x^{r-1}, y, yx, yx^2, \ldots, yx^{r-1}\}. \quad (1)$$

The main point in obtaining high order units is calculating the number of the units. This value can be determined by iterating through the elements, which requires significant computational effort. Indeed, taking an arbitrary element of a group ring, we must first find out whether it is a unit. Unlike group rings given by a finite field and a finite cyclic group, the Euclidean algorithm does not work in dihedral group rings. Therefore, we need to iterate over the powers of the element and see when we get 1. At the same time, we also obtain the order of the element if it is a unit. At the same time, the total number of q^{2r} elements of the ring $F_q[D_r]$ increases rapidly with increasing of the numbers q and r.

To reduce computational costs, it is proposed to use an algebraic approach. It consists in applying a combination of two fundamental results from the theory of algebraic structures.

On the one hand, the structure of semisimple rings is described by the Wedderburn-Artin theorem. The theorem states that any semisimple (artinian) ring is isomorphic to the direct sum of rings of matrices of size n_i by n_i with elements from the division ring D_i, where numbers n_i are uniquely defined, and division rings – up to isomorphism. In particular, a simple ring is isomorphic to a matrix ring over the division ring.

On the other hand, the Maschke theorem is a theorem in group representation theory regarding the decomposition of representations of finite groups into irreducible representations. The theorem allows us to draw conclusions about the representation of finite groups without calculating them. It reduces the problem of classifying all representations to the problem of classifying irreducible representations, the direct sum of which decomposes an arbitrary representation.

If F is a field and G a finite group with n elements, then the group ring $F[G]$ is semi simple if and only if the

field characteristic does not divide n. This result is known as Maschke theorem and is important in group representation theory. The conditions of Maschke theorem are satisfied by the group ring $F_a[D_r]$ if the characteristic of the field does not divide the number $2r$.

Combining both results, for the group ring $F_q[D_r]$ (the characteristic of the field F_q does not divide $2r$), we have that it is a direct sum of a finite number of complete matrix rings over division rings [13]:

$$R[G] \cong \bigoplus_{i=1}^{l} M_{n_i}(F_{q_i}), \qquad (2)$$

where numbers n_i and q_i are uniquely defined.

This means that each such ring can be represented as a direct sum of such elementary "building blocks" – matrix rings, and this representation is unique. Uniqueness of the decomposition – the decomposition into such blocks is unique up to the order of factors.

Based on this decomposition, the number of units in the group ring can be calculated as the product of numbers of units in each block. At the same time, one should also take into account the peculiarities of searching for high order units in each of factors.

If the number $n_i = 1$, i.e. the complete matrix ring reduces to a finite field, then all nonzero elements are units. The maximum possible order of an element is equal to the number of non-zero elements of the field. It is known that elements of the mentioned order always exist.

If the number $n_i > 1$, then the invertible elements of the complete matrix ring form the so called general linear group over a finite field. More precisely, take a natural number $n_i \geq 2$. One of the widely known non-abelian groups is the general linear group $GL(n_i, F_q)$ – matrices of size $n_i \times n_i$, which are filled with elements of the field F_q and with non-zero determinant, with respect to the matrix multiplication operation (or in another form linear transformations in one variant from $(F_q)^m$ to $(F_q)^m$, and in another variant – from F_{q^m} to F_{q^m}, with respect to the operation of composition of mappings). The number of elements of the group equals $|GL(n_i, F_q)| = \prod_{i=0}^{n_i-1}(q^{n_i} - q^i)$. It is shown (Cayley-Hamilton theorem) that the maximum possible order of an element in this group is equal to $q^{n_i} - 1$. It is also known that elements of the specified order always exist. They are commonly called Singer cycles. However, it is not known how to explicitly construct the mentioned elements in general.

The decomposition given earlier is a result about the existence. It is not clear from it how to actually get the decomposition. Results on how this can be done explicitly are not known for arbitrary pairs q and r. The corresponding description, provided that every prime divisor of the number r divides $q-1$, is given in [13, Theorem 4.4].

To verify the validity of theoretical constructions, in particular the mentioned description, we performed calculations in Python environment for various group rings that are given by a finite field and dihedral group. Some of the obtained results are given in Table 1. Comments and explanations for some rows of this table are provided after the table.

Actually, three fundamentally different cases were considered. In this case, we use the following notation: k is the greatest common divisor of the numbers r and $q-1$; $m = \frac{r}{k}$.

1. The case when number r is odd.

In this case, the decomposition has the block of the form $2F_q$, $\frac{k-1}{2}$ blocks of the form $M_2(F_q)$ and for every divisor t of the number m ($t \neq 1$) $\frac{k\varphi(t)}{2t}$ blocks of the form $M_2(F_{q^t})$.

Structure of Group Rings of the Form $F_q[D_r]$

q	r	***Structure of $F_q[D_r]$***
5	8	$4F_5 \oplus M_2(F_5) \oplus M_2(F_{5^2})$
5	32	$4F_5 \oplus M_2(F_5) \oplus M_2(F_{5^2}) \oplus M_2(F_{5^4}) \oplus M_2(F_{5^8})$
5	128	$4F_5 \oplus M_2(F_5) \oplus M_2(F_{5^2}) \oplus M_2(F_{5^4}) \oplus M_2(F_{5^8}) \oplus M_2(F_{5^{16}}) \oplus M_2(F_{5^{32}})$
7	6	$4F_7 \oplus 2M_2(F_7)$
7	54	$4F_7 \oplus 2M_2(F_7) \oplus 2M_2(F_{7^3}) \oplus 2M_2(F_{7^9})$
7	243	$2F_7 \oplus M_2(F_7) \oplus M_2(F_{7^3}) \oplus M_2(F_{7^9}) \oplus M_2(F_{7^{27}}) \oplus M_2(F_{7^{81}})$
9	128	$4F_9 \oplus 3M_2(F_9) \oplus 2M_2(F_{9^2}) \oplus 2M_2(F_{9^4}) \oplus 2M_2(F_{9^8}) \oplus 2M_2(F_{9^{16}})$
11	125	$2F_{11} \oplus 2M_2(F_{11}) \oplus 2M_2(F_{11^5}) \oplus 2M_2(F_{11^{25}})$
13	128	$4F_{13} \oplus M_2(F_{13}) \oplus M_2(F_{13^2}) \oplus M_2(F_{13^4}) \oplus M_2(F_{13^8}) \oplus M_2(F_{13^{16}}) \oplus M_2(F_{13^{32}})$
17	128	$4F_{17} \oplus 7M_2(F_{17}) \oplus 4M_2(F_{17^2}) \oplus 4M_2(F_{17^4}) \oplus 4M_2(F_{17^8})$

For example, take $q = 7$ and $r = 243$. Then there is the block $2F_7$ in the decomposition. Since $k = 3$, then $\frac{k-1}{2}=1$ and we have one block $M_2(F_7)$. As $m = 81$, then the non-1 divisors of this number are equal to 3, 9, 27 and 81. For each of these divisors t, the value of the expression $\frac{k\varphi(t)}{2t}$ is calculated. For all four values of divisors, the value of the expression is equal to 1. That is, we have in the decomposition one block $M_2(F_{7^3})$, $M_2(F_{7^9})$, $M_2(F_{7^{27}})$ and $M_2(F_{7^{81}})$ at a time.

Summarizing the above considerations, we obtained the following decomposition:

$$F_7[D_{243}] \cong 2F_7 \oplus M_2(F_7) \oplus M_2(F_{7^3}) \oplus M_2(F_{7^9}) \oplus M_2(F_{7^{27}}) \oplus M_2(F_{7^{81}}). \quad (3)$$

Based on the decomposition, we have the following number of units:

$$|F_7[D_{243}]^*| = 7^2 \cdot [(7^2-1)(7^2-7)] \cdot [(7^6-1)(7^6-7^3)] \cdot [(7^{18}-1)(7^{18}-7^9)] \cdot [(7^{54}-1)(7^{54}-7^{27})] \cdot [(7^{162}-1)\cdot(7^{162}-7^{81})]$$

2. The case when r is even and $q \equiv 1 (\mathrm{mod}\, 4)$ or 8 does not divide r.

The decomposition has the block of the form $4F_q$, $\frac{k}{2}-1$ blocks of the form $M_2(F_q)$ and for every divisor t of the number m, that is not equal to 1, $\frac{k\varphi(t)}{2t}$ blocks of the form $M_2(F_{q^t})$.

We took for example $q = 5$ and $r = 128$. Then there is the block $4F_5$ in the decomposition. Since $k = 4$, then $\frac{k}{2}-1=1$ and we have one block $M_2(F_5)$. As $m = 32$, then the non-1 divisors of this number are equal to 2, 4, 8, 16 and 32. For each of these divisors t, the value of the expression $\frac{k\varphi(t)}{2t}$ is calculated. For all five values of divisors, the value of the expression is equal to 1. That is, we have in the decomposition one block $M_2(F_{5^2})$, $M_2(F_{5^4})$, $M_2(F_{5^8})$, $M_2(F_{5^{16}})$ and $M_2(F_{5^{32}})$ at a time.

Summarizing the above considerations, we obtained the following decomposition:

$$F_5[D_{128}] \cong 4F_5 \oplus M_2(F_5) \oplus M_2(F_{5^2}) \oplus M_2(F_{5^4}) \oplus M_2(F_{5^8}) \oplus M_2(F_{5^{16}}) \oplus M_2(F_{5^{32}}). \quad (4)$$

Based on the decomposition, we have the following number of units:

$$|F_5[D_{128}]^*| = 4^4 \cdot [(5^2-1)(5^2-5)] \cdot [(5^4-1)(5^4-5^2)] \cdot [(5^8-1)(5^8-5^4)] \cdot [(5^{16}-1)(5^{16}-5^8)] \cdot [(5^{32}-1)\cdot(5^{32}-5^{16})] \cdot [(5^{64}-1)\cdot(5^{64}-5^{32})]$$

3. The case when r is even and $q \equiv 3 (\mathrm{mod}\, 4)$ and 8 divides r.

We use the following additional notation: $\nu = \min(\nu_2(\frac{r}{2}), \nu_2(q+1))$, $m' = \frac{r}{2^\nu k}$, the number i equals 0, if $\nu_2(q+1) > \nu_2(\frac{r}{2})$, and equals 1, if $\nu_2(q+1) \le \nu_2(\frac{r}{2})$.

In this case, the decomposition has the block of the form $4F_q$, $k + 2^{\nu-i} - 3$ blocks of the form $M_2(F_q)$, $2^{\nu-2}k - 2^{\nu-1} - \frac{k}{4} + 1$ blocks of the form $M_2(F_{q^2})$, for every odd divisor t of the number m' $(t \neq 1)$ $\frac{k\varphi(t)}{2t}$ blocks of the form $M_2(F_{q^t})$ and $\frac{(2^{\nu-1}-1)k\varphi(t)}{2t}$ blocks of the form $M_2(F_{q^{2t}})$, for every even divisor t of the number $m' - \frac{2^{\nu-2}k\varphi(t)}{t}$ blocks of the form $M_2(F_{q^{2t}})$.

After obtaining the number of elements, typical techniques should be applied: factoring the obtained number into prime factors and applying the corollary of Lagrange's theorem for finite groups.

Factor the number $|U(F_q[D_r])$ into prime factors. In general, the computational complexity of factoring a number is subexponential. However, for factors of a specific type that are present in this number, you can use ready-made tables from the Cunningham project (with Brent-Montgomery-te Riel additions). This is a project to factor numbers of the form $b^n \pm 1$. There are three printed versions of the tables, as well as an online version.

For example, in the case $q = 5$ and $r = 128$, we have the following factorizations into primes for divisors of the number $|U(F_q[D_r])$:

$5^{16} - 1 = 2^6 \cdot 3 \cdot 13 \cdot 17 \cdot 313 \cdot 11489$

$5^{16} - 5^8 = 2^5 \cdot 3 \cdot 5^8 \cdot 13 \cdot 313$

$5^{64} - 1 = 2^8 \cdot 3 \cdot 13 \cdot 17 \cdot 313 \cdot 641 \cdot 2593 \cdot 11489 \cdot 29423041 \cdot 75068993 \cdot 241931001601$

$5^{64} - 5^{32} = 2^7 \cdot 3 \cdot 5^{32} \cdot 13 \cdot 17 \cdot 313 \cdot 2593 \cdot 11489 \cdot 29423041$

$5^{128} - 1 = 2^9 \cdot 3 \cdot 13 \cdot 17 \cdot 313 \cdot 641 \cdot 769 \cdot 2593 \cdot 11489 \cdot 75068993 \cdot 29423041 \cdot 3666499598977 \cdot 241931001601 \cdot 961329567826437419512256640001$

$5^{128} - 5^{64} = 2^8 \cdot 3 \cdot 5^{64} \cdot 13 \cdot 17 \cdot 313 \cdot 641 \cdot 2593 \cdot 11489 \cdot 29423041 \cdot 75068993 \cdot 241931001601$

Randomly select element of the group ring. Applying corollary of Lagrange theorem for finite groups, find the order of the element. The formulation of this

corollary is that the order of any element of a finite group is a divisor of the number of elements of the group. If the element is not a unit (does not equal to the group identity in the power of any possible divisor) or a unit, but not of high order, then return to element selection.

V. CONCLUSION

To implement cryptosystems based on the discrete logarithm problem in group rings, it is necessary to find high order elements in these rings explicitly.

A method was proposed for obtaining units of high multiplicative order in group rings given by a finite field and a finite non-abelian dihedral group. The main point here was to calculate the number of units. To reduce computational costs, an algebraic approach should be used: decompose the group ring into a direct sum of a finite number of complete matrix rings over finite fields. Based on this decomposition, the number of units in the group ring can be calculated as the product of numbers of units in each block.

This method can be applied provided that the numbers q and $2r$ are coprime, and every prime divisor of the number r divides $q-1$. The limitation of the method is that it is not always possible to find the factorization of the number of group ring units.

VI. CONFLICTS OF INTEREST

The authors declare no conflicts of interest.

I. DECLARATION ON GENERATIVE AI

During the preparation of this work, the authors used ChatGPT, Google Translate in order to analyze and translate text between languages. After using these tools, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] Galbraith, S. D. (2018). Mathematics of public key cryptography, *Cambridge University Press*, 696.

[2] Jespers, E. (2021). Structure of group rings and the group of units of integral group rings: an invitation. *Indian J. Pure Appl Math. 52*(3), 687-708. DOI: https://doi.org/10.1007/s13226-021-00179-5.

[3] Hurley, B., & Hurley, T. (2011). Group ring cryptography. *Int. J. Pure Appl. Math.* 69(1), 67-86.

[4] Hurley, T. (2015). Group rings for communications. *Int. J. Group Theory.* 4(4), 1–23. DOI: https://doi.org/10.22108/IJGT.2015.5453.

[5] Mittal, G., Kumar, Sunil, Narain, S., & Kumar, Sandeep. (2022). Group ring based public key cryptosystems. *J. Discrete Math. Sci. Cryptogr.* 25(6), 1–22. DOI: https://doi.org/10.1080/09720529.2020.1796868.

[6] Creedon L., Hughes K., Szabo S. (2021). A comparison of group algebras of dihedral and quaternion groups. *Appl. Alg. Eng. Com. Comp.,* 32(1), 245-264. DOI: 10.1007/s00200-020-00485-1

[7] Cheng, Q., Zhang, J., & Zhuang, J. (2022). LWE from non-commutative group rings. *Des. Codes Cryptogr.* 90(4), 239–263. DOI: https://doi.org/10.1007/s10623-021-00973-6.

[8] Inam, S., Kanwal, S., & Ali, R. (2021). A new encryption scheme based on groupring. *Contem. Math.* 2(2), 103–112. DOI: 10.37256/cm.222021611.

[9] Makhlouf, S., & Guenda, K. (2023). A new public key cryptosystem based on group ring. *Adv. Math.* 12(2), 357–366. DOI: https://doi.org/10.37418/amsj.12.2.4.

[10] Oberyshyn, R., & Popovych, R. (2024). On units in one class of group ring, *Herald Khmelnytskyi National Univ. Tech. Sci.* 343(6(1)), 191–194. DOI: https://doi.org/10.31891/2307-5732-2024-343-6.

[11] Sahai, M., & Ansari, S. F. (2020). Unit groups of group algebras of certain dihedral groups, [Electronic resource]. Malaysian J. Math. Sci. 14(3): https://qsj-waf.upm.edu.my/lihatmakalah.php?kod=2020/September/14/3/419–436.

[12] Sharma, R. K., & Kumar, Y. (2024). The unit group of the group algebra F_qD_{36}, *J. Iran. Math, Soc.,* 5(1), 45–53. DOI: https://dx.doi.org/10.30504/JIMS.2024.405833.1131.

[13] Martinez, F. E. B. (2015). Structure of finite dihedral group algebra. *Finite Fields Appl.* 35, 204–214. DOI: https://doi.org/10.1016/j.ffa.2015.05.002.

Roksolana Oberyshyn was born in Lviv, Ukraine. She received the B.S. and M.S. degrees in computer engineering at Lviv Polytechnic University, Ukraine, in 2002. Since 2024 she has been a Senior Lecture, Department of Specialized Computer System at Lviv Polytechnic National University. Her research interests include algebra and number theory, cryptography.

.

Roman Popovych doctor of physical and mathematical sciences, professor, professor of the Department of Specialized Computer Systems at Lviv Polytechnic National University. He pursued postgraduate studies at Physics-Mechanics Institute, Lviv. He defended his candidate's thesis in the specialty information and measuring systems in 1988 and earned his Doctor degree in 2016. His research interests include algebra, number theory and their applications, cryptography, digital signal processing.