Hadamard Modulo Prime Matrices and Their Application in Cryptography: A Survey of Some Recent Works

Yuri L. Borissov

Abstract The notion of Hadamard modulo prime (HMP) matrix inherits in basics that of classical real Hadamard matrix. Namely, by definition, HMP modulo odd prime p matrix $\mathbf{H}$ of size n, is a $n \times n$ non-singular over $\mathbb{Z}_p$ matrix of ± 1's satisfying the equality: $\mathbf{H}\mathbf{H}^T = n(mod p)\,\mathbf{I}$ where $\mathbf{I}$ is the identity matrix of same size. The HMP matrices have an attractive application in the modern cryptography due to the fact of their efficient employment in constructing of some all-or-nothing transform schemes. The present paper surveys some recent results on this kind of matrices by revealing their connections with coding theory, combinatorics, and elementary number theory.

1 Introduction

The HMP matrices can be considered in the broader context of modular Hadamard matrices introduced by Marrero and Butson [1] in 1973. Notice as well that the concept of modular Hadamard matrices has recently resurfaced in the engineering literature during the course of investigation of jacket transforms [2].

In this paper, the focus of attention is on the prime modular matrices motivated by their important application in cryptography: the so-called all-or-nothing transform (AONT).

Usually, an AONT scheme is a public (non-confidential, keyless) preprocessing step when encrypting data with some block cipher encryption. Its essence consists of providing a certain amount of additional security over and above the block cipher encryption since to determine any one of the message blocks embedded by that

Y. L. Borissov (✉)
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
8 G. Bonchev Street, 1113 Sofia, Bulgaria
e-mail: youri@math.bas.bg

M. Chakraborty et al. (eds.), *Proceedings of International Ethical Hacking Conference 2018*, Advances in Intelligent Systems and Computing 811,
https://doi.org/10.1007/978-981-13-1544-2_1

transform into a single large block, the potential adversary has to break (somehow) all corresponding blocks of the cryptogram [3].

In [4] it is shown (among other things) how to construct an efficient AONT scheme of linear type by exploiting in appropriate way conventional real Hadamard matrix. Later on, the authors of [5] have proposed an extension of that construction employing instead of conventional matrix such a matrix of HMP type which enables the size not restricted to 2 or multiples of 4.

Recently, some newly obtained classification and (non-)existence results on matrices of the latter kind have been presented in [6] and [7]. On the other hand, the mathematical concept of AONT scheme has evolved as well (see, the newest articles [8, 9] devoted to that topic).

The outline of the present survey is as follows. In the next section, the necessary definitions and preliminary facts are recalled. In Sect. 3, some general results on HMP matrices, and in the subsequent section some results on HMP matrices whose size is relatively small with respect to their modulo, are exposed. In Sect. 5, the results concerning HMP matrices derived by the finite projective planes are exhibited. In Sect. 6, after a brief reminder of the basic concept and construction of AONT scheme presented in [4], it is indicated how matrices of the considered kind can be employed in such a scheme. Finally, some conclusions and directions for future research are drawn.

2 Preliminaries

Definition 1 ([5, 7]) A HMP modulo odd prime p matrix $\mathbf{H}$ of size n is a $n \times n$ non-singular over $\mathbb{Z}_p$ matrix of ± 1's such that

$$\mathbf{H}\mathbf{H}^T = n(mod\ p)\ \mathbf{I}, \tag{1}$$

where $\mathbf{I}$ is the identity matrix of size n.

As usual, $\mathbf{H}^T$ denotes the transpose matrix of a given matrix $\mathbf{H}$. Also, further on $HMP(n, p)$ stands for the set of HMP modulo p matrices of size n.

It is necessary to set out two simple but essential remarks.

Remark 1 Although some authors do not impose invertibility on the (modular) matrices considered [6], I prefer to do because of the aforesaid application of corresponding linear transforms. A necessary and sufficient condition for that is the matrix size n not to be a multiple of the chosen modulo p. So, further on it is always assumed that $p \neq n$.

Remark 2 Apparently, each conventional Hadamard matrix is a HMP modulo arbitrary prime $p > 2$ matrix, provided p does not divide the matrix size.

Example 1 The simplest non-trivial HMP matrix is obtained for $n = 7$, $p = 3$, e.g.,

$$\begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & - & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & - \\ \mathbf{1} & \mathbf{1} & - & \mathbf{1} & \mathbf{1} & \mathbf{1} & - \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & - & \mathbf{1} & \mathbf{1} & - \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & - & \mathbf{1} & - \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & - & - \\ \mathbf{1} & - & - & - & - & - & \mathbf{1} \end{pmatrix},$$

where—has been written instead of -1.

It is easy to see that by permuting the rows/columns or multiplying a row/column with -1 of a HMP matrix one gets again HMP matrix. This motivates the following definition relevant in the context of Hadamard matrices (see, e.g., [10, Ch. 14]).

Definition 2 The matrix $\mathbf{A}$ of ± 1s is called equivalent to the matrix $\mathbf{B}$ if the former is obtained from the latter by the following transformations:

- permuting the set of rows/columns of $\mathbf{B}$;
- multiplying each row/column from a certain subset of rows/columns in $\mathbf{B}$ with -1.

Remark 3 W.l.o.g. when performing these equivalence transformations one can apply at the beginning all permutations and then all transformations of the second kind (for details consult [7]).

3 Some Constructions of HMP Matrices

The results exposed in this section are from [5, 6].

First, a construction of HMP matrices which extends Example 1 is described.

Construction 1 *Let* $\mathbf{E}_n$ *where* $n = pk + 4, k \geq 0$, *be a square matrix of size* n *consisting of* ± 1*'s with the following description: its first row and column consist entirely of* 1*'s; its last row and column consist of* -1*'s with exception of the corner entries, and all other entries besides those on the main diagonal are equal to* 1. *Notice that* $\mathbf{E}_4$ *is the Sylvester-type Hadamard matrix of size* 4.

The proof that $\mathbf{E}_n$ is a HMP modulo prime p matrix is straightforward [5]. By multiplying the last row and column with -1 and then swapping the first and last column, one deduces that the matrix $\mathbf{E}_n$ is equivalent to the "diagonal" matrix $\mathbf{D}_n = \mathbf{J} - 2\mathbf{I}$ where $\mathbf{J}$ and $\mathbf{I}$ are the all-ones matrix and the identity matrix, respectively, both of size n.

Analogously to the case of conventional Hadamard matrices, the Kronecker product of two HMP modulo the same prime matrices of sizes n and m is a HMP matrix of

size nm. This property allows starting from the matrix $\mathbf{G}_1 = \mathbf{E}_q$, $q = p + 4$, to construct an infinite sequence of odd size HMP matrices defined recursively by: $\mathbf{G}_t = \mathbf{G}_1 \otimes \mathbf{G}_{t-1}$, $t \geq 2$. Clearly, for the size of $\mathbf{G}_t$ it holds: $q^t \ (mod \ p) = 4^t \ (mod \ p)$, and of course, the set $\{4^t \ (mod \ p) | \ t \geq 1\}$ is a subset of the set QR_p of quadratic residues modulo p. Some sufficient conditions for the prime p such that these two sets coincide (i.e., the order of 4 in the group $\mathbb{Z}_p^*$ to be equal to $|QR_p| = (p-1)/2$), are presented in [5] as follows:

Proposition 1 *Let p' be a prime number.*

- *if $p = 2p' + 1$ is also a prime number then $ord_p(4) = (p-1)/2$;*
- *if $p = 4p' + 1$ is also a prime number then $ord_p(4) = (p-1)/2$.*

The proof of Proposition 1 is based on facts which can be found, e.g., in [11, p. 123, p. 197].

Remark 4 An odd prime p is called a Sophie Germain prime if $2p + 1$ is also a prime. The first few S. Germain primes are: 3, 5, 11, 23, 29, 41, 53, 83, 113, 131, ... If both p and $4p + 1$ are primes, p is called sometimes a Stern prime. The first few such primes are: 3, 7, 13, 37, ...

The next necessary condition for the existence of HMP matrix of odd size is well-known.

Proposition 2 *[5] If the size n of HMP modulo p matrix is odd, then $n(mod \ p) \in QR_p$.*

Consider the case $p = 3$. Then the above proposition implies that for odd n the set $HMP(n, 3)$ can be non-empty only if $n \ (mod \ 6) = 1$. In fact, Construction 1 provides for any such n the matrix $\mathbf{E}_n \in HMP(n, 3)$ when k is odd. The even size case is split into two subcases: for $n \ (mod \ 6) = 4$ the same construction provides HMP matrix whenever k is even; while for $n \ (mod \ 6) = 2$, $n > 2$, a matrix of this kind can be constructed by the Kronecker product of Hadamard matrix of size 2 and $\mathbf{E}_{n/2}$. Results of similar type about 5−modular Hadamard matrices are presented in [6], where it is shown that such matrices do exist if and only if the size n satisfies constraints: $n \ (mod \ 10) \neq 3, 7$ or $n \neq 6, 11$.

Remark 5 Proposition 2 can be generalized for the m−modular Hadamard matrices of odd size n whenever n and m are co-primes (see, [6, Lemma 2.2] or earlier [1, Th 2.2]).

4 HMP Matrices of Small Size with Respect to Their Modulo

For basic definitions and facts from coding theory, the reader is referred to [12]. The classification and (non-)existence results about HMP matrices of the type considered in this section and obtained in [7] are based on the following two lesser-known facts:

(Hereinafter, $dist(\mathbf{x}, \mathbf{y})$ denotes the (Hamming) distance between the two vectors $\mathbf{x}$ and $\mathbf{y}$ of ± 1s while $wt(\mathbf{x}) \stackrel{\triangle}{=} dist(\mathbf{x}, \mathbf{1})$, where $\mathbf{1}$ is the all-ones vector, is called weight of $\mathbf{x}$.)

- **observation for parity**: For the (real) inner product of any two length n vectors $\mathbf{x}$ and $\mathbf{y}$ of ± 1s, it holds: $(\mathbf{x}, \mathbf{y}) = n - 2dist(\mathbf{x}, \mathbf{y})$, so $(\mathbf{x}, \mathbf{y}) \equiv n \ (mod\ 2)$;
- **intersection lemma**: For any two vectors $\mathbf{x}$ and $\mathbf{y}$ of ± 1s with same length, it holds: $dist(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} * \mathbf{y})$, where $\mathbf{x} * \mathbf{y}$ is the vector having -1s only where both $\mathbf{x}$ and $\mathbf{y}$ do.

The first proposition to pay attention is the following.

Proposition 3 *Let $\mathbf{H} \in HMP(n, p)$, where $n \leq p + 1$. Then $\mathbf{H}$ is a conventional Hadamard matrix.*

Corollary 1 *If $p \equiv 1(mod\ 4)$, then the set $HMP(p + 1, p)$ is the empty one.*

Proof When $p \equiv 1\ (mod\ 4)$ the existence of conventional Hadamard matrix of size $n = p + 1$ contradicts the well-known fact that n must be 1, 2, or $n \equiv 0(mod\ 4)$ (see, e.g., [13, Sect. 2.2]). □

Example 2 In particular, the above corollary implies that there does not exist $HMP(6, 5)$ matrix. The interested reader is referred to [6] for another proof of this particular case.

The next proposition considers HMP matrices of even sizes less than twice the modulo.

Proposition 4 *Let $\mathbf{H} \in HMP(n, p)$, where n is an even number such that $n < 2p$. Then $\mathbf{H}$ is a conventional Hadamard matrix.*

The proof of Proposition 4 given in [7] is based on the observation for parity. Correspondingly, it holds:

Corollary 2 *If $2 < n < 2p$ and $n \equiv 2(mod\ 4)$, then $HMP(n, p)$ is the empty set.*

Next, an assertion with respect to odd size HMP matrices extending a bit the region where that size varies is given by the following.

Proposition 5 *Let $\mathbf{H} \in HMP(n, p)$, where n is an odd number such that $n < 3p$, and let $\omega = (n - p)/2$. Then the matrix $\mathbf{H}$ is equivalent to a matrix $\mathbf{M}$ having the following properties:*

(i) the first row of $\mathbf{M}$ is the all-ones vector $\mathbf{1}$ (i.e., $\mathbf{M}$ is a normalized matrix);

(ii) all remaining rows are of weight ω;

(iii) for arbitrary two distinct rows $\mathbf{r}'$ and $\mathbf{r}''$ of $\mathbf{M}$, it holds: $dist(\mathbf{r}', \mathbf{r}'') = \omega$.

In addition, $n - p \equiv 0\ (mod\ 4)$ and $wt(\mathbf{r}' * \mathbf{r}'') = \omega/2$.

The proof of Proposition 5 given in [7] makes use of both the observation for parity and the intersection lemma. An immediate consequence is the following.

Corollary 3 *The set* $HMP(p+2l,\ p)$*, where* $l \equiv 1(mod\ 2)$ *and* $1 \leq l < p$*, is the empty one for arbitrary prime* p*.*

In particular,

Corollary 4 *If* $p \equiv 1(mod\ 4)$ *then* $HMP(2p+1,\ p) = \emptyset$*; If* $p \equiv 3(mod\ 4)$*, then* $HMP(2p-1,\ p) = \emptyset$*.*

Example 3 The set $HMP(11, 5)$ is the empty one (see, also [6] about that case).

Remark 6 The first claim of Corollary 4 cannot be inferred by Proposition 2 because 1 is always quadratic residue, while the second could be as well derived by that proposition since -1 is a quadratic non-residue modulo $p \equiv 3\ (mod\ 4)$.

Remark 7 Properties (iii)–(ii) from Proposition 5 mean that the binary code behind the rows (excepting the first one) of the matrix $\mathbf{M}$ is an equidistant constant weight code. Note, as well, that a theorem on the equivalence of a conventional Hadamard matrix of any admissible size and a certain constant weight binary code was proved in [14].

Proposition 3 shows the non-existence of matrices in $HMP(n,\ p)$ apart from the conventional ones when $n \leq p+1$. And, putting $l = 1$ in Corollary 3, it is concluded that $HMP(p+2,\ p)$ is empty for each p. Further, the case of even size $p+3$ (except the trivial $p = 3$) is managed by Proposition 4. So, the simplest case when a HMP matrix distinct from conventional one may exist is that of size $p+4$. Observe that the matrix $\mathbf{D}_{p+4}$, equivalent to the matrix $\mathbf{E}_{p+4}$ given by Construction 1, is an instance of $p+4$ size matrix. Finally, the following theorem completely characterizes all HMP matrices of this size.

Theorem 1 ([7]) *Let* $n = p+4$ *where* p *is an odd prime. Then*
(i) Every $\mathbf{H} \in HMP(n,\ p)$ *is equivalent to the matrix* $\mathbf{D}_n$*;*
(ii) The cardinality of $HMP(n,\ p)$ *equals to* $2^{2n-1}\ n!$

For the proof of this theorem, based on Proposition 5 and Remark 3, the interested reader is referred to [7].

Remark 8 A careful analysis of the proofs of Propositions 4, 5, and Theorem 1 shows that their assertions remain valid if instead of prime p it is put an arbitrary odd modulo m, while Proposition 3 is true for any invertible modular matrix.

5 HMP Matrices Derived by Finite Projective Planes

For basic definitions and facts about the finite projective planes, the reader is referred to [13, Sect. 1.2] or [15, Sect. 13.3.2]. Herein, for his/her convenience, recall the following:

Theorem 2 *Let $(\mathcal{P}, \mathcal{L})$ be a finite projective plane with $\mathcal{P}$ and $\mathcal{L}$ being the sets of its points and lines, respectively. Then there exists a constant s, called order of the plane, such that:*

- *Every line contains exactly $s + 1$ points;*
- *Every point lies on exactly $s + 1$ lines;*
- $|\mathcal{P}| = |\mathcal{L}| = v = s^2 + s + 1$.

Let $P_1, P_2, \ldots, P_v$; $l_1, l_2, \ldots, l_v$ be lists of the points and lines (arranged in some way) in the finite projective plane $(\mathcal{P}, \mathcal{L})$ of order s.

Definition 3 A binary $v \times v$ matrix $\mathcal{I} = (b_{km})$ with entry $b_{km} = 1$ if and only if the point $P_m \in l_k$ is called incidence matrix of the finite projective plane $(\mathcal{P}, \mathcal{L})$.

The matrix obtained from $\mathcal{I}$ by replacing 1 with -1 and 0 with 1 will be referred as $(-\mathbf{1}, \mathbf{1})-$image of the matrix $\mathcal{I}$.

Proposition 6 *The $(-\mathbf{1}, \mathbf{1})$-image of incidence matrix of a finite projective plane of order $s > 3$ is a HMP matrix modulo any prime factor of $s^2 - 3s + 1$.*

The proof follows by Theorem 2 and the definition of finite projective plane which together imply that the rows of incidence matrix constitute an equidistant constant weight code with parameters: length v, weight $s + 1$, and distance $2s$.

It is necessary to remind some background from elementary number theory in order to set out further results on HMP matrices considered in this section.
A particular case of the well-known law of quadratic reciprocity (see, e.g., Sect. 6 in [16]) is the following fact.

Lemma 1 *The number 5 is a quadratic residue modulo odd prime p if and only if $p \equiv \pm 1 \pmod{10}$.*

Recall also that the famous Dirichlet's theorem on primes in arithmetic progressions (see, e.g., [17, p. 16, Th. 15]) states that a progression $a + dt$, $t = 0, 1, \ldots$ with two positive co-prime integers a and d contains infinitely many primes.

Lemma 2 ([7]) *Let $T(x) = x^2 - 3x + 1$.*

(i) If p is a prime factor of $T(s)$ for some integer $s > 3$, then p is either equal to 5 or $p \equiv \pm 1 \pmod{10}$;

(ii) For any prime p either equal to 5 or $p \equiv \pm 1 \pmod{10}$, there exist infinite many primes q's such that p divides $T(q)$.

The proof of claim (i) is based on some elementary number-theoretic considerations and Lemma 1 while that of (ii) relies, in addition, on the Dirichlet prime number theorem.

The main result of this section is the following theorem.

Theorem 3 ([7]) *For $p = 5$ or any prime p of the form $p \equiv \pm 1 \pmod{10}$, there exist infinite class of HMP modulo p matrices each one of them being the $(-\mathbf{1}, \mathbf{1})-$image of incidence matrix of some finite projective plane of prime order.*

Table 1 HMP matrices derived by finite projective planes of prime orders ≤31

Order	5	7	11	13	17	19	23	29	31
Size	31	57	133	183	307	381	553	871	993
Modulo	11	29	89	131	239	5, 61	461	5, 151	11, 79

The proof is carried out taking into consideration Proposition 6, Lemma 2, and the existence of finite projective plane of order arbitrary prime power (see, e.g., [15, Sect. 13.3.2] for a construction).

For the prime numbers in the interval [5, 31]considered as orders of finite projective planes, Table 1 presents the corresponding sizes of HMP matrices with all possible modulus.

6 Application of HMP Matrices in Some AONT Schemes

Hereinafter, it is given a brief reminder of the description of all-or-nothing transform (AONT) scheme presented in [4].

Let X be a finite set, called alphabet. Let n be a positive integer, and suppose that $\phi : X^n \to X^n$, i.e., ϕ maps an input $n-$tuple, say $\mathbf{x} = (x_1, \ldots, x_n)$ to an output $n-$tuple, say $\mathbf{y} = (y_1, \ldots, y_n)$, where $x_i, y_i \in X$ for $1 \leq i \leq n$. Informally, the mapping ϕ is an *all-or-nothing transform* provided that the following properties are satisfied:

- ϕ is a bijection;
- If the values of any $n-1$ of the output variables $y_1, \ldots, y_n$ are fixed, then the value of each one input variable x_i, $(1 \leq i \leq n)$ is completely undetermined.

The mapping ϕ is referred as to a $(n, v)-$AONT, where $v = |X|$.

In [4], D.R. Stinson has given an easy method of constructing unconditionally secure linear AONT by the following theorem.

Theorem 4 ([4], 2001) *Suppose that q is a prime power, and $\mathbf{M}$ is an invertible square matrix of size n with entries from the field $\mathbb{F}_q$, such that no entry of $\mathbf{M}$ is equal to 0. Then the mapping $\phi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ defined by $\phi(\mathbf{x}) = \mathbf{x}\mathbf{M}^{-1}$ is a linear $(n, q)-$AONT.*

As an illustration of his method, Stinson has presented example of a linear $(n, p)-$AONT, for $n \equiv 0 \ mod \ 4$ and p odd prime, where in place of the matrix $\mathbf{M}$ is taken a conventional Hadamard matrix of size n with entries reduced to modulo p.
The contribution of [5] to the topic of interest can be expressed by the following:

Claim 1 ([5]) *The existence of HMP matrices (and corresponding constructions present so far) with sizes $\not\equiv 0 \ mod \ 4$ affords the scope of the aforesaid AONTs to be extended, e.g., for odd sizes. Also, note that such an AONT scheme is highly efficient*

requiring only additions, subtractions and (eventually) multiplication by constant modulo prime and even can provide opportunity to apply fast transform if such an algorithm is available.

7 Conclusion

As it is pointed out in [6], dealing with several exceptional cases of relatively small size and presenting infinite constructions of HMP matrices initialized in the surveyed works might be non-trivial in principal. An example in this direction is the infinite class of odd size HMP matrices derivable from finite projective planes and presented in [7].

The HMP matrices inherit the useful properties of the classical Hadamard matrices. However, an advantage in applications might be the existence among them of such species whose sizes are not restricted to multiples of 4. For instance, the employment of HMP matrix instead of conventional Hadamard in implementation of AONT scheme can extend essentially the scope of that cryptographic application while keeping its efficiency.

Acknowledgements The author is grateful to Prof. Moon Ho Lee for his helpful discussions on this topic and hospitality of the Department of Electrical and Electronics Engineering of Chonbuk National University, Republic of Korea, where most of this research was done during the years 2010–2012.

References

1. Marrero, O., Butson, A.T.: Modular Hadamard matrices and related designs. J. Comb. Theory A **15**, 257–269 (1973)
2. Lee, M.H.: A new reverse jacket transform and its fast algorithm. IEEE Trans. Circuits Syst. II **47**(6), 39–47 (2000)
3. Rivest, R.L.: All-or-nothing encryption and the package transform. In: Biham, E. (ed.) Fast Software Encryption. Lecture Notes Computer Science, vol. 1267, pp. 210–218 (1997)
4. Stinson, D.R.: Something about all or nothing (transforms). Des. Codes Cryptogr. **22**, 133–138 (2001)
5. Lee, M.H., Borissov, Y.L., Dodunekov, S.M.: Class of jacket matrices over finite characteristic fields. Electron. Lett. **46**(13), 916–918 (2010)
6. Lee, M.H., Szollosi, F.: Hadamard matrices modulo 5. J. Comb. Des. 171–178 (2013)
7. Borissov, Y.L.: Some new results on Hadamard modulo prime matrices. Probl. Inf. Transm. **52**(2), 134–141 (2016)
8. D'Arco, P., Nasr Esfahani, N., Stinson, D.R.: All or nothing at all. Electron. J. Comb. **23**(4), paper # P4.10, 24 pp (2016)
9. Nasr Esfahani, N., Goldberg, I., Stinson, D.R.: Some results on the existence of t-all-or-nothing transforms over arbitrary alphabets. IACR Cryptol. ePrint Archive **177** (2017)
10. Hall, M.: Combinatorial Theory. Blaisdell Publishing Company (1967)
11. Cusick, T.W., Ding, C., Revall, A.: Stream Ciphers and Number Theory. Elsevier, Amsterdam, The Netherlands (2004)

12. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-correcting Codes. North-Holland Publishing Company (1977)
13. Tonchev, V.D.: Combinatorial Configurations: Designs, Codes, Graphs. Longman Scientific & Technical (1988)
14. Zinoviev, V.A.: On the equivalence of certain constant weight codes and combinatorial designs. J. Stat. Plan. Inference **56**(2), 289–294 (1996)
15. van Tilborg, H.C.A.: Fundamentals of Cryptology, a Professional Reference and Interactive Tutorial. Kluwer Academic Publishers, Boston, Dordrecht, London (2000)
16. Vinogradov, I.M.: Elements of Number Theory (translated from the fifth revised edition by Saul Kravetz), 227 pp. Dover Publications Inc., Mineola, N.Y. (1954)
17. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers, 6th edn. Clarendon Press, Oxford, England (2008)