Asymptotic Behavior of the Ratio Between the Numbers of Binary Primitive and Irreducible Polynomials

Yuri Borissov[1] and Moon Ho Lee[2] and Svetla Nikova[3]

[1] Institute of Mathematics and Informatics
Bulgarian Academy of Sciences,
8 G.Bonchev, 1113 Sofia, Bulgaria
yborisov@moi.math.bas.bg
[2] Institute of Information and Communication,
Chonbuk National University
Jeonju 561-756, R. Korea
moonho@chonbuk.ac.kr
[3] ESAT/SCD/COSIC, Katholieke Universiteit Leuven, Belgium
svetla.nikova@esat.kuleuven.be

Abstract.
In this paper we study the ratio $\theta(n) = \frac{\lambda_2(n)}{\psi_2(n)}$, where $\lambda_2(n)$ is the number of primitive polynomials and $\psi_2(n)$ is the number of irreducible polynomials in $GF(2)[x]$ of degree n. Let $n = \prod_{i=1}^{\ell} p_i^{r_i}$ be the prime factorization of n, where p_i are odd primes. We show that $\theta(n)$ tends to 1 and $\theta(2n)$ is asymptotically not less than $2/3$ when r_i are fixed and p_i tend to infinity. We also, describe an infinite series of values n_s such that $\theta(n_s)$ is strictly less than $\frac{1}{2}$.

1 Introduction

One of the most fascinating areas of research in the theory of finite fields is the problem of finding irreducible and primitive polynomials (or elements), and even the problem of the existence of such kind of polynomials with specified properties has attracted a great deal of attention. Many authors have published works on this subject (see [5] –[8], [11] – [12], [17] – [22] and [25] – [26]) and the list might not be complete. Motivated by the recent proposals in design of stream ciphers ([1], [2] and [10]), in this paper we consider and investigate to some extent the problem of the existence of primitive polynomials in $GF(2)[\mathbf{x}]$ of degree powers of prime numbers, for which the substitution $\mathbf{x} \mapsto \mathbf{x} + 1$ leads again to primitive polynomial. Our results can be interpreted probabilistically: to estimate the probability of a randomly chosen irreducible polynomial in $GF(2)[\mathbf{x}]$ of given degree to be primitive.

The paper is organized as follows. In the first section we recall basic definitions, facts and useful properties. In the next two sections we present our main results. The paper ends with some conclusions.

2 Background

In this paper we consider polynomials of one variable $\mathbf{x}$ over a finite field. Here, for the sake of completeness, we briefly recall some basic definitions and facts about polynomials in $GF(q)[\mathbf{x}]$, where $GF(q)$ is the Galois field of q elements (see e.g., [14],[24]).

Definition 1. *A polynomial $f(\mathbf{x})$ is irreducible in $GF(q)[\mathbf{x}]$ if $f(\mathbf{x})$ cannot be factored into a product of lower-degree polynomials in $GF(q)[\mathbf{x}]$.*

It can be shown that any irreducible nth-degree polynomial in $GF(q)[\mathbf{x}]$ divides $\mathbf{x}^{q^n-1}-1$.

Definition 2. *An irreducible polynomial $f(\mathbf{x}) \in \mathbf{GF(q)}[\mathbf{x}]$ of degree n is said to be primitive if the smallest positive integer m for which $f(\mathbf{x})$ divides $\mathbf{x}^m-1$ is $m=q^n-1$.*

By definition a primitive polynomial $f(\mathbf{x}) \in GF(q)[\mathbf{x}]$ is always irreducible in $GF(q)[\mathbf{x}]$, but the opposite not always holds i.e. there exist irreducible polynomials which are not primitive. As a simple example, consider the polynomial $\mathbf{x}^4+\mathbf{x}^3+\mathbf{x}^2+\mathbf{x}+1$, which is irreducible in $GF(2)[\mathbf{x}]$, but as a factor of $\mathbf{x}^5+1$, it is not primitive.

Let denote by $M_n = 2^n-1$ the $n-$th Mersenne number. From now on, we will consider only the binary polynomials, i.e., over $GF(2)$.

Definition 3. *The dual of an irreducible polynomial $f(\mathbf{x}) \in GF(2)[\mathbf{x}]$, denoted by $f^{\perp}(\mathbf{x})$, is the polynomial $f(\mathbf{x}+1)$.*

It is easy to prove that $f(\mathbf{x})$ is a binary irreducible polynomial if and only if its dual $f^{\perp}(\mathbf{x})$ is irreducible. However, the duality operator does not necessarily preserve being primitive. As a simple example, consider the primitive polynomial $\mathbf{x}^4+\mathbf{x}^3+1$ whose dual polynomial is $\mathbf{x}^4+\mathbf{x}^3+\mathbf{x}^2+\mathbf{x}+1$, but the latter is not primitive as already mentioned.

The number of irreducible polynomials in $GF(2)[\mathbf{x}]$ of degree n is given by (see e.g., [3, 13]):

$$\psi_2(n) = \frac{1}{n}\sum_{d|n} 2^d \mu(\frac{n}{d}), \tag{1}$$

where μ is the well-known Möbius function (i.e., if N is a positive integer, the Möbius function $\mu(N)$, is 0 if p^2 divides N for some prime p; 1 if N is square free and contains an even number of prime factors; and -1 if N is square free and contains an odd number of prime factors; a literal interpretation gives $\mu(1)=1$).

While the number of binary primitive polynomials of degree n is given by:

$$\lambda_2(n) = \frac{\Phi(2^n-1)}{n}, \tag{2}$$

where Φ is the Euler function (i.e., $\Phi(N)$ is the number of positive integers smaller than N and relatively prime to N).

We shall also make use of the following lemma:

Lemma 1. *For any n the number of binary irreducible polynomials $\psi_2(n)$ does not exceed $(2^n-2)/n$, where the equality holds when n is a prime.*

Proof. The statement of Lemma 1 follows from the fact that the greatest two powers of 2 in formula (1) are obtained when we take as divisors, n itself, and its second largest divisor d in which case the quotient n/d is a prime number. □

Note that if $n = p^r$ (for p a prime number), we obtain $\psi_2(p^r) = 2^{p^r} - 2^{p^{r-1}}$.

In this paper we study the ratios

$$\theta(n) = \frac{\lambda_2(n)}{\psi_2(n)} \quad \text{and} \quad \tau(n) = \frac{\Phi(2^n-1)}{2^n-1}. \tag{3}$$

Since $\psi_2(n) \le (2^n-2)/n < M_n/n$, we have $\theta(n) > \tau(n)$ for any $n > 1$. On the other hand since every primitive polynomial is irreducible, clearly we have that $\lambda_2(n) \le \psi_2(n)$, i.e., $\theta(n) \le 1$. Hence the following relations hold

$$1 \ge \theta(n) > \tau(n) > 0. \tag{4}$$

In [4] the following proposition has been proven, using a simple form of the principle of inclusion-exclusion from elementary combinatorics:

Proposition 1. *If $\theta(n) > \frac{1}{2}$ then there exist at least $2\lambda_2(n) - \psi_2(n)$ primitive polynomials of degree n such that their duals are primitive too.*

According to the table with the values of λ_2 and ψ_2 for $n = 2 \dots 24$ in [13, p.40], the only values of n for which the assumptions of Proposition 1 are not satisfied are $n = 12$ and $n = 20$. By computer simulations we obtained the results given in Table 1. In this table $\sigma_2(n)$ denotes the number of primitive polynomials of degree n, the duals of which are primitive too. Note that when M_p is Mersenne prime number, any irreducible polynomial of degree p is primitive and therefore $\sigma_2(p) = \lambda_2(p)$ when $p = 2, 3, 5, 7$ and 13. In [4], based on Proposition 1 some estimates on the number of the above mentioned primitive polynomials of an arbitrary prime degree and of degree, which is a product of two distinct primes were proven.

Proposition 2. *[4] For any odd primes $p \ge p_0$ and $q \ge q_0$, we have:*

$$\theta(p) \ge E(p_0), \qquad \tau(2p) > \frac{2}{3}E^2(p_0) \quad \textit{and} \quad \tau(pq) > E(p_0)E(q_0)E(p_0q_0), \tag{5}$$

where $E(y) = e^{-\frac{1}{2\lg(2y+1)}}$ for a positive integer y and e is the base of the natural logarithm.

Since $E(2)$ and $\frac{2}{3}E^2(7)$ are greater than $\frac{1}{2}$ and since $\lim_{p_0\to\infty} E(p_0) = 1$ the following Corollary holds.

Corollary 1. *[4] For any prime number p there exist primitive polynomials of degree $n = p$ and primitive polynomial of degree $n = 2p$ such that their duals are primitive too.*
For sufficiently large primes p and q almost all irreducible polynomials of degree $n = p$ and $n = pq$ are primitive.

n	σ_2	λ_2	ψ_2
2	1	1	1
3	2	2	2
4	1	2	3
5	6	6	6
6	3	6	9
7	18	18	18
8	9	16	30
9	42	48	56
10	35	60	99
11	166	176	186
12	55	144	335
13	630	630	630
14	486	756	1161
15	1486	1800	2182
16	1011	2048	4080

Table 1. Values of σ_2, λ_2, ψ_2

3 Estimations on $\tau(\prod_{i=1}^{\ell} p_i^{r_i})$ and $\tau(2^{r_0}\prod_{i=1}^{\ell} p_i^{r_i})$

First of all we will recall some facts from elementary Number Theory [23]. Let $GCD(a,m)=1$. By the Euler theorem we have $a^{\phi(m)} \equiv 1(\mathrm{mod}\ m)$. Based on this it is defined the index to which a belongs modulo m to be the smallest $\delta > 0$ such that $a^{\delta} \equiv 1(\mathrm{mod}\ m)$. It is easy to prove that a belongs to δ modulo m if and only if δ divides any γ for which $a^{\gamma} \equiv 1(\mathrm{mod}\ m)$. In particular the index δ divides $\phi(m)$.

Theorem 1. *Let r_i $(i=1,\ldots,\ell)$ be some positive integers. Then for any odd primes $p_i \geq \tilde{p}_i$ $(i=1,\ldots,\ell)$, we have:*

$$\tau(\prod_{i=1}^{\ell} p_i^{r_i}) > \exp\left(-\frac{1}{2}\sum_{(j_1,\ldots,j_\ell)\preceq(r_1,\ldots,r_\ell)} \frac{1}{\lg(2\prod_{i=1}^{\ell}\tilde{p}_i^{\,j_i}+1)}\right). \tag{6}$$

Proof. Let us denote by $Q_{(k_1,\ldots,k_\ell)}$ the set of prime factors of $M_{\prod_{i=1}^{\ell} p_i^{k_i}}$, where $(k_1,\ldots,k_\ell)$ is a $\ell-$tuple of integers such that $(k_1,\ldots,k_\ell) \preceq (r_1,\ldots,r_\ell)$. Let q be an arbitrary element from $Q_{(r_1,\ldots,r_\ell)}$, (i.e., q is a prime such that $2^{\prod_{i=1}^{\ell} p_i^{r_i}} \equiv 1(\mathrm{mod}\ q)$) and δ be the index to which 2 belongs modulo q. By the above general considerations it follows that δ is a divisor of both $\prod_{i=1}^{\ell} p_i^{r_i}$ and $\phi(q)=q-1$, i.e., there exists a tuple of integers $(j_1,\ldots,j_\ell) \preceq (r_1,\ldots,r_\ell)$, such that $\delta = \prod_{i=1}^{\ell} p_i^{j_i}$ and $q = 2m\delta+1$ for some positive m. It is easy to see that q belongs to $Q_{(j_1,\ldots,j_\ell)} \setminus \cup_{(k_1,\ldots,k_\ell)\prec(j_1,\ldots,j_\ell)} Q_{(k_1,\ldots,k_\ell)}$. We will denote the last set by $N_{(j_1,\ldots,j_\ell)}$ and let $n_{(j_1,\ldots,j_\ell)}$ be its cardinality.

First, let us give an upper bound on $n_{(j_1,\ldots,j_\ell)}$. Although more precise estimations of $n_{(j_1,\ldots,j_\ell)}$ might be possible, for our goals it is sufficient the following.

Since for any $q \in N_{(j_1,\ldots,j_\ell)}, q \geq 2\prod_{i=1}^{\ell} p_i^{j_i} + 1$ holds, then

$$2^{\prod_{i=1}^{\ell} p_i^{j_i}} > M_{\prod_{i=1}^{\ell} p_i^{j_i}} > \prod_{q \in N_{(j_1,\ldots,j_\ell)}} q \geq \left(2\prod_{i=1}^{\ell} p_i^{j_i} + 1\right)^{n_{(j_1,\ldots,j_\ell)}}.$$

Taking logarithm base 2, we get: $\prod_{i=1}^{\ell} p_i^{j_i} > n_{(j_1,\ldots,j_\ell)} \lg(2\prod_{i=1}^{\ell} p_i^{j_i} + 1)$ or $n_{(j_1,\ldots,j_\ell)} < \frac{\prod_{i=1}^{\ell} p_i^{j_i}}{\lg(2\prod_{i=1}^{\ell} p_i^{j_i}+1)} < \frac{\prod_{i=1}^{\ell} p_i^{j_i}}{\lg(2\prod_{i=1}^{\ell} \tilde{p_i}^{j_i}+1)}$. Let us denote by $L_{(j_1,\ldots,j_\ell)} = \frac{1}{\lg(2\prod_{i=1}^{\ell} \tilde{p_i}^{j_i}+1)}$, so we have:

$$n_{(j_1,\ldots,j_\ell)} < L_{(j_1,\ldots,j_\ell)} \prod_{i=1}^{\ell} p_i^{j_i}, \tag{7}$$

where $L_{(j_1,\ldots,j_\ell)}$ does not depend on p_i.
Let $\pi_{(j_1,\ldots,j_\ell)} = \prod_{q \in N_{(j_1,\ldots,j_\ell)}} (1 - \frac{1}{q})$. Replacing every q by the lower bound $2\prod_{i=1}^{\ell} p_i^{j_i} + 1$ and taking into account (7), we get:

$$\begin{aligned}
\pi_{(j_1,\ldots,j_\ell)} &> (1 - \frac{1}{2\prod_{i=1}^{\ell} p_i^{j_i} + 1})^{L_{(j_1,\ldots,j_\ell)} \prod_{i=1}^{\ell} p_i^{j_i}} \\
&= (1 + \frac{1}{2\prod_{i=1}^{\ell} p_i^{j_i}})^{-L_{(j_1,\ldots,j_\ell)} \prod_{i=1}^{\ell} p_i^{j_i}} \\
&= \left[(1 + \frac{1}{2\prod_{i=1}^{\ell} p_i^{j_i}})^{2\prod_{i=1}^{\ell} p_i^{j_i}}\right]^{-\frac{1}{2}L_{(j_1,\ldots,j_\ell)}}
\end{aligned}$$

Since the inequality $(1 + \frac{1}{n})^n < e$, where e is the base of natural logarithm holds for every positive integer n, it follows that:

$$\pi_{(j_1,\ldots,j_\ell)} > e^{-\frac{1}{2}L_{(j_1,\ldots,j_\ell)}} \tag{8}$$

The following computations are straightforward:

$$\begin{aligned}
\tau(\prod_{i=1}^{\ell} p_i^{r_i}) = \frac{\Phi(M_{\prod_{i=1}^{\ell} p_i^{r_i}})}{M_{\prod_{i=1}^{\ell} p_i^{r_i}}} &= \prod_{q \in Q_{(r_1,\ldots,r_\ell)}} (1 - \frac{1}{q}) \qquad (9) \\
&= \prod_{(j_1,\ldots,j_\ell) \prec (r_1,\ldots,r_\ell)} \tau(\prod_{i=1}^{\ell} p_i^{j_i}) \prod_{q \in N_{(r_1,\ldots,r_\ell)}} (1 - \frac{1}{q}) \\
&= \prod_{(j_1,\ldots,j_\ell) \prec (r_1,\ldots,r_\ell)} \tau(\prod_{i=1}^{\ell} p_i^{j_i}) \pi_{(r_1,\ldots,r_\ell)} \\
&= \prod_{(j_1,\ldots,j_\ell) \preceq (r_1,\ldots,r_\ell)} \pi_{(j_1,\ldots,j_\ell)}.
\end{aligned}$$

Then from (8) we get the following lower bound on $\tau(\prod_{i=1}^{\ell} p_i^{r_i})$:

$$\tau(\prod_{i=1}^{\ell} p_i^{r_i}) > e^{-\frac{1}{2}\sum_{(j_1,\ldots,j_\ell)\preceq(r_1,\ldots,r_\ell)} \frac{1}{\lg(2\prod_{i=1}^{\ell}\tilde{p_i}^{j_i}+1)}}, \tag{10}$$

which is the desired result. □

Corollary 2. *For any fixed positive integers r_i $(i = 1, \ldots, \ell)$ and sufficiently large primes p_i, almost all irreducible polynomials of degree $\prod_{i=1}^{\ell} p_i^{r_i}$ are primitive.*

Proof. Since $\theta(n) > \tau(n)$ for any n, in particular the ratio $\theta(\prod_{i=1}^{\ell} p_i^{r_i})$ is greater than $\tau(\prod_{i=1}^{\ell} p_i^{r_i})$. But the latter becomes greater than any constant $c < 1$ when p_i are chosen sufficiently large according to the lower bound proved. □

Remark 1. Note, that under the assumptions of Corollary 2 it follows by the same reasoning that almost all elements of the multiplicative group of the finite field $GF(2^{\prod_{i=1}^{\ell} p_i^{r_i}})$ are primitive (i.e., of maximal possible order).

Now we will consider the case when the degree of the polynomial is $2^{r_0}n$, where n is an odd number with prime factorization $n = \prod_{i=1}^{\ell} p_i^{r_i}$ and $r_0 \geq 1$.

Theorem 2. *Let $r_0 \geq 0$ and $r_i\,(i = 1, \ldots, \ell)$ be some positive integers. Then for any odd primes $p_i \geq \tilde{p_i}$ $(i = 1, \ldots, \ell)$, we have:*

$$\tau(2^{r_0}\prod_{i=1}^{\ell} p_i^{r_i}) > \tau(2^{r_0})\exp\left(-2^{r_0-1}\sum_{(j_1,\ldots,j_\ell)\preceq(r_1,\ldots,r_\ell)} \frac{1}{\lg(2\prod_{i=1}^{\ell}\tilde{p_i}^{j_i}+1)}\right). \tag{11}$$

Proof. The proof is by induction on r_0. The case $r_0 = 0$ is in fact statement of Theorem 1 and gives the base of induction. The inductive step can be drawn by the following arguments. Since:

$$2^{2^{r+1}n} - 1 = (2^{2^r n} - 1)(2^{2^r n} + 1)$$

the prime factors of $2^{2^r n} + 1$ are prime factors of $2^{2^{r+1}n} - 1$. Thus, the index δ of 2 modulo such prime factor is either equal to 2^{r+1} or of the form $2^{r+1}\prod_{i=1}^{\ell} p_i^{j_i}$ for some $(j_1, \ldots, j_\ell) \preceq (r_1, \ldots, r_\ell)$, where not all j_i are equal to 0. The prime factors of the first type contribute to $\tau(2^{r+1})$, while the contribution of those of the second type can be estimated in the same way as the corresponding prime factors of $2^{2^r n} - 1$, since they are of the form $m\delta + 1 = 2m\,2^r\prod_{i=1}^{\ell} p_i^{j_i} + 1$ for some positive m. □

To illustrate the consequences of Theorem 2 we formulate the following corollary, which is derived from case $r_0 = 1$.

Corollary 3. *For any fixed positive integers r_i $(i = 1, \ldots, \ell)$ and sufficiently large primes p_i, not less than $2/3$ of all irreducible polynomials of degree $2\prod_{i=1}^{\ell} p_i^{r_i}$ are primitive.*

Example 1. As it follows from Proposition 1 the interesting case is when $\tau(n) > \frac{1}{2}$. Straightforward calculations show that in order to have inequality $\tau(p^r) > \frac{1}{2}$, for $1 \leq r \leq 4$, it is sufficient to choose $\tilde{p} = 3$. In other words for all prime numbers p we have $\tau(p^r) > \frac{1}{2}$ when $1 \leq r \leq 4$. To add the case $r = 5$, we should choose $\tilde{p} = 5$ and the inequalities $\tau(2^5) > \frac{1}{2}$ and $\tau(3^5) > \frac{1}{2}$ can be checked directly.

4 An infinite series of integers n_s for which $\theta(n_s) < \frac{1}{2}$

We will prove the following proposition.

Proposition 3. *There exists an infinite series of integers $n_s = 2^s, s \geq 7$ for which the number of primitive polynomials of degree n_s is strictly less than the half of the number of irreducible polynomials of that degree.*

Proof. The following computations are straightforward:

$$2^{2^s} - 1 = (2^{2^{s-1}})^2 - 1 = (2^{2^{s-1}} - 1)(2^{2^{s-1}} + 1)$$

and since $GCD(2^{2^{s-1}} - 1, 2^{2^{s-1}} + 1) = 1$ we have:

$$\tau(2^s) = \frac{\Phi(2^{2^s} - 1)}{2^{2^s} - 1} = \frac{\Phi(2^{2^{s-1}} - 1)}{2^{2^{s-1}} - 1} \cdot \frac{\Phi(2^{2^{s-1}} + 1)}{2^{2^{s-1}} + 1} < \frac{\Phi(2^{2^{s-1}} - 1)}{2^{2^{s-1}} - 1} = \tau(2^{s-1})$$

Direct calculations show that $\tau(64) < \frac{1}{2}$ and hence $\tau(2^s) < \frac{1}{2}$ when $s \geq 6$. So for $s > 6$, it follows that:

$$\Phi(2^{2^s} - 1) = \Phi(2^{2^{s-1}} - 1) \cdot \Phi(2^{2^{s-1}} + 1) < \frac{1}{2}(2^{2^{s-1}} - 1)2^{2^{s-1}}.$$

On the other hand we have that: $\psi_2(2^s) = \sum_{d|2^s} 2^d \mu(\frac{2^s}{d}) = (2^{2^{s-1}} - 1)2^{2^{s-1}}$ and from the above inequality if $s > 6$ we get:

$$\theta(2^s) = \frac{\Phi(2^{2^s} - 1)}{(2^{2^{s-1}} - 1)2^{2^{s-1}}} < \frac{1}{2}.$$

□

Recently, in papers by Luka, Luka and Shparlinski and J. von zur Gathen et.al., [9, 15, 16] similar ratios of multiplicative number-theoretical functions have been studied from a more general point of view (the usage of groups in cryptography). Their results show that the mean behavior of these functions is limited by well determined constants and that there exist infinite series of integers for which these ratios take the largest possible value as well as relatively small values. We believe our results complete in certain aspects the results of these papers giving different and constructive examples of such series.

5 Conclusions

Based on number-theoretic considerations we present estimations on the ratio between the number of primitive and irreducible polynomials of degrees n and $2n$, for an arbitrary odd n. As a consequence we prove that when the powers (in the prime factorization of n) are fixed and the primes are sufficiently large, almost (2/3 of) all binary irreducible polynomials of these degrees are primitive, respectively. Then we show that for any prime number p and $1 \leq r \leq 5$, there exists a primitive polynomial of degree p^r such that its dual is primitive, too.

Finally, we describe infinite series of degrees (namely $n_s = 2^s, s \geq 7$) for which the number of primitive polynomials in $GF(2)[\mathbf{x}]$ is strictly less than $\frac{1}{2}$ of the number of corresponding irreducible polynomials.

References

1. S. Babbage, M. Dodd, "Finding Characteristic Polynomials with Jump Indices", IACR e-Print Archive 2006/010.
2. S. Babbage, M. Dodd, "MICKEY, eSTREAM - the ECRYPT Stream Cipher Project", http://www.ecrypt.eu.org/stream/mickey.html.
3. E. Berlekamp, "Algebraic Coding Theory", McGraw-Hill, New York, 1968.
4. Y. Borissov, S. Nikova, N. Manev, "On primitive polynomials over GF(2) the duals of which are also primitive", in Proc. of the Twenty-Seventh Symposium on Information Theory in the Benelux, pp. 221-226, 2006.
5. R. Brent, "Searching for primitive trinomials (mod 2)", homepage of R. Brent.
6. S.D. Cohen, "Primitive polynomials with a prescribed coefficient", Finite Fields Appl., 12, pp. 425-491, 2006.
7. S.D. Cohen, D. Mills, "Primitive polynomials with first and second coefficients prescribed", Finite Fields and Their Applications 9 (3), pp. 334–350, 2003.
8. S. Dodunekov, "Essentially different irreducible polynomials over finite fields", Ann. University of Sofia, Faculty of Mathematics and Mechanics 1971, 66, pp. 169-175.
9. J. von zur Gathen, A. Knopfmacher, L. G. Lucht, F. Luca, I. E. Shparlinski, "Average order in cyclic groups", J. Théorie des Nombres Bordeaux, 16, 2004, pp. 107–123
10. C.J.A. Jansen, "Stream cipher design based on jumping finite state mashines", IACR e-print Archive 2005/267.
11. J. von zur Gathen: "Irreducible trinomials over finite fields", ISSAC 2001, pp. 332–336
12. J. von zur Gathen, I. Shparlinski, "Constructing Elements of Large Order in Finite Fields", AAECC 1999, pp. 404–409.
13. S.W. Golomb, "Shift register Sequences", Aegen Park press, 1982.
14. R. Lidl, H. Niderreiter, "Introduction to Finite Fields and their Applications", Cambridge University Press, 1994.
15. F. Luca, "Some mean values related to average multiplicative orders of elements in finite fields", Ramanujan J. of Math., 9, 2005, pp. 33–44.
16. F. Luca and I. E. Shparlinski, "Average multiplicative orders of elements modulo n", Acta Arith., 109, 2003, pp. 387–411.
17. J. Lucas, G. Mullen, "Irreducible polynomials over GF(2) with prescribed coefficients", Discrete Mathematics 274 (1-3), pp. 265–279, 2004.

18. O. Moreno, "On Primitive Elements of Trace equal to 1 in $GF(2^m)^*$", Discrete Mathematics 41 (1), pp. 53-56, 1982.
19. M. Rabin. Probabilistic algorithms in finite fields, SIAM J. Comput. 9, pp. 273-280, 1980.
20. V. Shoup, Searching for primitive roots in finite fields, Math. Comp. 58, pp. 369–380, 1992.
21. I. Shparlinski, "On Irreducible Polynomials of Small Height over Finite Fields", Appl. Algebra Eng. Commun. Comput. 7 (6), pp. 427–431, 1996.
22. I. Shparlinski, "Finding Irreducible and Primitive Polynomials", Appl. Algebra Eng. Commun. Comput. 4, pp. 263–268, 1993.
23. I. Vinogradov, "Basics of Number Theory", Moscow 1972, Publishing House Nauka (in Russian).
24. S. Wicker, "Error Control Systems for Digital Communication and Storage", Prentice Hall International, Inc., 1995.
25. N. Zierler, J. Brillhart, "On Primitive Trinomials (mod 2)", Information and Control 13 (6), pp. 541-554, 1968.
26. N. Zierler, "Primitive Trinomials Whose Degree is a Mersenne Exponent", Information and Control 15 (1), pp. 67-69, 1969.