UDC 512.772.7 DOI 10.17223/20710410/37/2

HYPERELLIPTIC CURVES, CARTIER — MANIN MATRICES AND LEGENDRE POLYNOMIALS

S. A. Novoselov

Immanuel Kant Baltic Federal University, Kaliningrad, Russia

Using hyperelliptic curves in cryptography requires the computation of the Jacobian order of a curve. This is equivalent to computing the characteristic polynomial of Frobenius $\chi(\lambda) \in \mathbb{Z}[\lambda]$. By calculating Cartier — Manin matrix, we can recover the polynomial $\chi(\lambda)$ modulo the characteristic of the base field. This information can further be used for recovering full polynomial in combination with other methods. In this paper, we investigate the hyperelliptic curves of the form $C_1 : y^2 = x^{2g+1} + ax^{g+1} + bx$ and $C_2 : y^2 = x^{2g+2} + ax^{g+1} + b$ over the finite field $\mathbb{F}_q$, $q = p^n$, $p > 2$. We transform these curves to the form $C_{1,\rho} : y^2 = x^{2g+1} - 2\rho x^{g+1} + x$ and $C_{2,\rho} : y^2 = x^{2g+2} - 2\rho x^{g+1} + 1$, where $\rho = -a/(2\sqrt{b})$, and prove that the coefficients of the corresponding Cartier — Manin matrices for the curves in this form are Legendre polynomials. As a consequence, the matrices are centrosymmetric and therefore, for finding the matrix, it's enough to compute a half of coefficients. Cartier — Manin matrices are determined up to a transformation of the form $S^{(p)}WS^{-1}$. It is known that centrosymmetric matrices can be transformed to the block-diagonal form by an orthogonal transformation. We prove that this transformation can be modified to have a form $S^{(p)}WS^{-1}$ and be defined over the base field of the curve. Therefore, Cartier — Manin matrices of curves $C_{1,\rho}$ and $C_{2,\rho}$ are equivalent to block-diagonal matrices. In the case of $\gcd(p, g) = 1$, Miller and Lubin proved that the matrices of curves C_1 and C_2 are monomial. We prove that the polynomial $\chi(\lambda) \pmod p$ can be found in factored form in terms of Legendre polynomials by using permutation attached to the monomial matrix. As an application of our results, we list all possible polynomials $\chi(\lambda) \pmod p$ in the case of $\gcd(p, g) = 1$, g is from 2 to 7 and the curve C_1 is over $\mathbb{F}_p$ if $\sqrt{b} \in \mathbb{F}_p$ and over $\mathbb{F}_{p^2}$ if $\sqrt{b} \notin \mathbb{F}_p$.

Keywords: *hyperelliptic curve cryptography, Cartier — Manin matrix, Legendre polynomials.*

Introduction

Let $\mathbb{F}_q$ be a finite field, $q = p^n$, $p > 2$. A hyperelliptic curve of a genus g over $\mathbb{F}_q$ is a nonsingular curve given by an equation

$$C : y^2 = f(x),$$

where $f \in \mathbb{F}_q[x]$, f is monic, $\deg f = 2g + 1$ or $\deg f = 2g + 2$.

Hyperelliptic curves were first proposed for use in cryptography by Koblitz [1]. Due to index-calculus attacks on hyperelliptic curves [2–4], only curves with a small genus are now considered in cryptography. In the more specific area of the cryptography on pairings, we are only interested in curves over prime and possibly medium or big characteristic fields, since in this case the security of cryptosystems relies on the discrete logarithm problem in finite fields, which has quasi-polynomial complexity for finite fields with a small characteristic [5].

The hyperelliptic curve C has an associated group — its Jacobian $J_C(\mathbb{F}_q)$, where all computations take place. For applications in cryptography, we need to compute the order

of $J_C(\mathbb{F}_q)$. Computing the order of Jacobian is equivalent to computing characteristic polynomial $\chi_q(\lambda)$ of the Frobenius endomorphism of J_C, which is determined by zeta function. If $N_k = \#C(\mathbb{F}_{q^k})$, then zeta function is a generating function

$$Z(\lambda) := \exp\left(\sum_{k=1}^{\infty} \frac{N_k}{k}\lambda^k\right) = \frac{L(\lambda)}{(1-\lambda)(1-q\lambda)},$$

where $L(\lambda) \in \mathbb{Z}[\lambda]$ is the L-polynomial, $L(\lambda) = \lambda^{2g}\chi_q(1/\lambda)$, and we have $\#J_C(\mathbb{F}_q) = \chi_q(1) = L(1)$.

Let $f(x)^{(p-1)/2} = \sum\limits_{i=0}^{(\deg f)(p-1)/2} c_i x^i$. Then Cartier — Manin matrix of the hyperelliptic curve C is a matrix

$$W = (w_{ij}) = \begin{pmatrix} c_{p-1} & c_{p-2} & \dots & c_{p-g} \\ c_{2p-1} & c_{2p-2} & \dots & c_{2p-g} \\ \dots & \dots & \dots & \dots \\ c_{gp-1} & c_{gp-2} & \dots & c_{gp-g} \end{pmatrix}.$$

Manin [6] showed that the characteristic polynomial of the matrix W is connected with the polynomial $\chi_q(\lambda)$ in the following way. Let $W_p = W \cdot W^{(p)} \cdot \ldots \cdot W^{(p^{n-1})}$, where $W^{(p^k)} = (w_{i,j}^{p^k})$, then

$$\chi_q(\lambda) \equiv (-1)^g \lambda^g |W_p - \lambda I_g| \pmod{p}.$$

Cartier — Manin matrices can in general be computed by optimized algorithms from [7, 8], which are faster than collecting coefficients after expansion of $f(x)^{(p-1)/2}$. After computing the polynomial $\chi_q(\lambda) \bmod p$, we can use Hasse — Weil bound in combination with other methods to recover full polynomial $\chi_q(\lambda)$.

In this work, we study hyperelliptic curves of the form

$$C_1 : y^2 = x^{2g+1} + ax^{g+1} + bx$$

and

$$C_2 : y^2 = x^{2g+2} + ax^{g+1} + b.$$

These curves are isomorphic to curves

$$C_{1,\rho} : y^2 = x^{2g+1} - 2\rho x^{g+1} + x$$

and

$$C_{2,\rho} : y^2 = x^{2g+2} - 2\rho x^{g+1} + 1$$

over the field $K = \mathbb{F}_q[\sqrt{b}]$. Therefore, we can restrict the discussion to the curves $C_{1,\rho}$ and $C_{2,\rho}$ and our results for polynomials $\chi(\lambda)$ hold over $\mathbb{F}_q$ if b is a square and over $\mathbb{F}_{q^2}$ if b is not a square in $\mathbb{F}_q$. These forms of curves are motivated by Jacobi quartics investigated by N. Yui [9].

The curves C_1 and C_2 were first studied by Miller and Lubin [10, 11], who proved that the Cartier — Manin matrices of these curves are the generalized permutation (monomial) matrices.

F. Leprevost and F. Morain [12] expressed the number of points of these curves in terms of certain modular functions, which can be efficiently computed for some special instances of curves.

For $g = 1$ these curves are elliptic ones. It is known that the number of points of elliptic curves in Legendre form for C_1 and Jacobi form for C_2 is congruent to Legendre polynomials

(see [9, 13] for details). Here, we show that this can be generalized to $g > 1$ case and prove that the number of points in J_{C_1} and J_{C_2} is congruent to an expression in terms of Legendre polynomials.

The genus 2 case was investigated for use in cryptography in [14 – 16]. It was proved that the genus 2 curves of the forms C_1 and C_2 have Jacobian isogenous to direct product of elliptic curves. Some explicit formulas for zeta function and for $\chi_q(\lambda)$ were found.

In this paper, we list all the possibilities for the polynomial $\chi_q(\lambda)$ modulo prime p for genus g from 2 to 7, $p > 2$, $\gcd(p, g) = 1$, and the curve C_1 over $\mathbb{F}_p$ if $b \in \mathbb{F}_p$ (Table 1) and over $\mathbb{F}_{p^2}$ if $b \notin \mathbb{F}_p$ (Table 2). Our methods can also be applied to any genus and finite field $\mathbb{F}_{p^n}$ with $\gcd(p, g) = 1$ and $p > 2$.

The rest of the paper is organized as follows. In section 1.1, we collect and prove preliminary results for monomial matrices and their permutations. In section 1.2, we prove necessary conditions for coefficients of Cartier — Manin matrices of C_1 and C_2 to be non-zero. From this, we also obtain conditions for the matrix to be diagonal or anti-diagonal.

In section 2.1, we prove that non-zero elements of Cartier — Manin matrix of the curve C_1 are Legendre polynomials and, as consequence, that the matrix is centrosymmetric. Using this fact, we prove that Cartier — Manin matrix of the curve C_1 is equivalent to a block-diagonal matrix over the finite field $\mathbb{F}_q$. In the case when the matrix is monomial with an attached permutation σ, we show how the polynomial $\chi_q(\lambda) \pmod p$ can be found in factored form by using this permutation and methods from Section 1.1. Section 2.2 contains analogous results for the curve C_2.

Tables 1 and 2 contain all the possible variants of the polynomials $\chi(\lambda) \pmod p$ for the case of $\gcd(g, p) = 1$, $p > 2$, and the curve C_1 over the fields $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$.

1. Preliminary results

1.1. Permutations specified by congruence

A matrix M of size $n \times n$ is a generalized permutation (or monomial) matrix if each its column as well as each its row contains exactly one non-vanishing element. Every such a matrix can be decomposed into the product of a diagonal matrix and a permutation matrix

$$M = \operatorname{diag}(m_1, m_2, \ldots, m_n)P_\sigma$$

for some permutation $\sigma \in \operatorname{Sym}(n)$. Consider the case when the permutation σ is defined by a congruence modulo n.

Theorem 1. Let a, b, n be integers, $n > 1$, $a \not\equiv 1 \pmod n$, $\gcd(a, n) = 1$, $M = \operatorname{diag}(m_1, m_2, \ldots, m_n)P_\sigma$ be a monomial matrix, and σ be a permutation such that $\sigma(i) \equiv ai - b \pmod n$. Then

1) $\sigma^s(i) \equiv a^s i - b\left(\dfrac{a^s - 1}{a - 1}\right) \pmod n$;
2) $\operatorname{ord}(\sigma) = \operatorname{ord}_n(a)$;
3) if $d_j = \gcd(a^j - 1, n)$ and $b_j = b\left(\dfrac{a^j - 1}{a - 1}\right)$, then the number of cycles in the decomposition of the permutation σ into disjunct cycles equals

$$m = \frac{1}{\operatorname{ord}_n(a)}\left(n + \sum_{d_j | b_j} d_j\right),\ 1 \leqslant j \leqslant \operatorname{ord}_n(a) - 1;$$

4) if $\sigma = \sigma_1\sigma_2\dots\sigma_m$ is the disjunct cycles decomposition of σ, then the characteristic polynomial $\chi_M(\lambda)$ of the matrix M factors in the following way:

$$\chi_M(\lambda) = \prod_{j=1}^{m} (\lambda^{|\sigma_j|} - m_{\sigma_j}),$$

where m_{σ_j} is the product of all elements in the matrix M with indexes in the cycle σ_j.

Proof.

1) Let $s = 1$. Then $\sigma(i) \equiv ai - b\left(\dfrac{a-1}{a-1}\right) \pmod n$. Let $s+1 > 1$. Then

$$\sigma^{s+1}(i) = \sigma(\sigma^s(i)) \equiv a\left(a^s i - b\left(\frac{a^s-1}{a-1}\right)\right) - b \equiv a^{s+1}i - b\left(\frac{a^{s+1}-1}{a-1}\right) \pmod n.$$

So the formula is true by induction.

2) Let $r = \mathrm{ord}_n(a)$. Assume that there exists $j < r$ such that $\sigma^j(i) = i$ for all i. Then for all i, we have

$$(a^j - 1)i \equiv b\left(\frac{a^j-1}{a-1}\right) \pmod n.$$

This congruence has solutions iff $\gcd(a^j - 1, n) = d_j | b\left(\dfrac{a^j-1}{a-1}\right)$; in this case, the number of solutions is equal to d_j.

Since r is the minimal integer such that $a^r \equiv 1 \pmod n$, we have $a^j \not\equiv 1 \pmod n$. Then $d_j < n$ and there exists integer j_0 such that $\sigma^j(j_0) \not\equiv j_0 \pmod n$. This contradiction proves our statement.

3) Cycles in the disjunct decomposition of the permutation σ correspond to orbits in the action of the group $\langle\sigma\rangle$ on the set $S = \{1, \dots, n\}$.

The number of orbits can be calculated by Burnside's lemma:

$$m = \frac{1}{|\langle\sigma\rangle|}\sum_{j=1}^{|\langle\sigma\rangle|} \#\{i \in S : \sigma^j(i) = i\} = \frac{1}{r}\left(n + \sum_{j=1}^{r-1} \#\{i \in S : \sigma^j(i) = i\}\right).$$

The number of elements i such that $\sigma^j(i) = i$ is equal to the number of solutions of the congruence $a^j i - b\left(\dfrac{a^j-1}{a-1}\right) \equiv i \pmod n$, which is $d_j = \gcd(a^j - 1, n)$ if $d_j \Big| b\left(\dfrac{a^j-1}{a-1}\right)$ and 0 otherwise. Therefore,

$$m = \frac{1}{r}\left(n + \sum_{d_j | b_j} d_j\right).$$

4) See [17, Theorem 3]. ■

1.2. Hyperelliptic curves of the form $y^2 = x^t + ax^s + bx^m$

The next lemma gives some necessary conditions for coefficients of the Cartier — Manin matrix of a named form curve to be zero.

Lemma 1. Let $C : y^2 = x^t + ax^s + bx^m$ be a genus g hyperelliptic curve over finite field $\mathbb{F}_q$, $q = p^n$, $p > 2$, $t \in \{2g+2, 2g+1\}$, $m < s < t$, $m \in \{0, 1\}$ and $d = \gcd(t-m, s-m)$. Let $W = (w_{i,j})$, $1 \leqslant i, j \leqslant g$, be the Cartier — Manin matrix of the curve C. Then $w_{i,j} = 0$ for all i, j such that $ip - j \not\equiv m(p-1)/2 \pmod d$.

Proof. We have

$$w_{i,j} = [x^{ip-j}](x^t + ax^s + bx^m)^{(p-1)/2} = [x^{ip-j-m(p-1)/2}](x^{t-m} + ax^{s-m} + b)^{(p-1)/2} =$$
$$= [x^{ip-j-m(p-1)/2}] \sum_{k_1+k_2+k_3=(p-1)/2} \binom{(p-1)/2}{k_1, k_2, k_3} a^{k_2} b^{k_3} x^{(t-m)k_1+(s-m)k_2} = \sum_{k_1,k_2,k_3} \binom{(p-1)/2}{k_1, k_2, k_3} a^{k_2} b^{k_3},$$

where sum goes all k_1, k_2, k_3, which satisfy the system of equations

$$\begin{cases} k_1 + k_2 + k_3 = (p-1)/2, \\ (t-m)k_1 + (s-m)k_2 = ip - j - m(p-1)/2. \end{cases}$$

The second equation has a solution in integers k_1, k_2 if and only if $\gcd(t-m, s-m)$ divides $ip - j - m(p-1)/2$. Otherwise, the system has no solutions and we get $w_{i,j} = 0$. ■

From this lemma, we obtain some sufficient conditions for the Cartier — Manin matrix to be diagonal or anti-diagonal.

Theorem 2. Let $C : y^2 = x^{2g+1} + ax^{g+1} + bx$ be a genus g hyperelliptic curve over the finite field $\mathbb{F}_q$ and W be the Cartier — Manin matrix of this curve. Then

1) W is a diagonal matrix if one of the following conditions holds:
   a) g is even and $p \equiv 1 \pmod{2g}$;
   b) g is odd and $p \equiv 1 \pmod{g}$.
2) W is a anti-diagonal matrix if one of the following conditions holds:
   a) g is even and $p \equiv -1 \pmod{2g}$;
   b) g is odd and $p \equiv -1 \pmod{g}$.

Proof.

1) Let g be even and $p \equiv 1 \pmod{2g}$. Then $p = 1+2gm$ for some integer m. By Lemma 1 elements of matrix W can be non-zero only if $g|(ip - j - (p-1)/2) = i(1+2gm) - j - gm$, i.e. should be $i \equiv j \pmod{g}$. Since $1 \leqslant i, j \leqslant g$, we get $i = j$.

Let g be odd and $p \equiv 1 \pmod{g}$. Since $\gcd(g, 2) = 1$, $ip - j - (p-1)/2 \equiv i - j \pmod{g}$ and $i \equiv j \pmod{g}$.

2) The proof is similar to 1. ■

2. Main results

2.1. Curves of the form $y^2 = x^{2g+1} + ax^{g+1} + bx$

The genus g hyperelliptic curves of the form $C_1 : y^2 = x^{2g+1} + ax^{g+1} + bx$ over the finite field $\mathbb{F}_q$ are isomorphic over $\mathbb{F}_q[\sqrt{b}]$ to

$$C_{1,\rho} : y^2 = x^{2g+1} - 2\rho x^{g+1} + x, \ \rho = -\frac{a}{2\sqrt{b}}$$

via isomorphism

$$(x, y) \mapsto \left(b^{1/(2g)} x, b^{(2g+1)/(4g)} y\right).$$

Let $K = \mathbb{F}_q[\sqrt{b}]$. If b is a square in $\mathbb{F}_q$, then $K = \mathbb{F}_q$, otherwise $K \cong \mathbb{F}_{q^2}$.

First, we proof that the coefficients of the Cartier — Manin matrix W of the curve $C_{1,\rho}$ correspond to the Legendre polynomials.

Theorem 3. Let $C_{1,\rho} : y^2 = x^{2g+1} - 2\rho x^{g+1} + x$ be a genus g hyperelliptic curve over the finite field $\mathbb{F}_q$ and $W = (w_{i,j})$ be the Cartier — Manin matrix of $C_{1,\rho}$. Then

1) $w_{i,j} = 0$, if $ip - j \not\equiv (p-1)/2 \pmod{g}$;

2) $w_{i,j} \equiv P_{(ip-j)/g-(p-1)/(2g)}(\rho) \pmod p$, otherwise.

Proof.

1) The statement follows from Lemma 1.

2) Let $ip - j \equiv (p-1)/2 \pmod g$ and therefore $g|(ip - j - (p-1)/2)$. We have

$$w_{i,j} = \left[x^{ip-j-(p-1)/2}\right] (x^{2g} - 2\rho x^g + 1)^{(p-1)/2}.$$

Making substitution $z = x^g$, we get

$$w_{i,j} = \left[z^{(ip-j)/g-(p-1)/(2g)}\right] (z^2 - 2\rho z + 1)^{(p-1)/2} \equiv \left[z^{(ip-j)/g-(p-1)/(2g)}\right] \frac{1}{\sqrt{z^2 - 2\rho z + 1}} \pmod p.$$

Note that the generating function of the Legendre polynomials has the form

$$\sum_{k=0}^{\infty} P_k(x) z^k = \frac{1}{\sqrt{z^2 - 2xz + 1}}.$$

From this, it follows that $w_{i,j} \equiv P_{(ip-j)/g-(p-1)/(2g)}(\rho)$. ■

In many cases, the Cartier — Manin matrix of the curve $C_{1,\rho}$ has some special forms. We collect and prove these ones in the following theorem.

Theorem 4. Let $y^2 = x^{2g+1} - 2\rho x^{g+1} + x$ be a genus g hyperelliptic curve over the field $\mathbb{F}_q$ and W be the Cartier — Manin matrix of the curve. Then matrix W is

1) centrosymmetric in $\mathbb{F}_q$;
2) monomial, if $\gcd(p, g) = 1$;
3) diagonal, if one of the following conditions holds:
   a) g is even and $p \equiv 1 \pmod{2g}$;
   b) g is odd and $p \equiv 1 \pmod g$;
4) antidiagonal, if one of the following conditions holds:
   a) g is even and $p \equiv -1 \pmod{2g}$;
   a) g is odd and $p \equiv -1 \pmod g$.

Proof.

1) By Theorem 3, when $g|(ip - j - (p-1)/2)$ we have

$$w_{i,j} \equiv P_{(ip-j)/g-(p-1)/(2g)}(\rho) \pmod p.$$

From congruence properties of the Legendre polynomials [18, (5.9)], we get

$$P_{p-1-m}(\rho) \equiv P_m(\rho) \pmod p,\ 0 \leqslant m \leqslant p-1.$$

So

$$w_{i,j} \equiv P_{(ip-j)/g-(p-1)/(2g)}(\rho) \equiv P_{p-1-(ip-j)/g+(p-1)/(2g)}(\rho) \equiv$$
$$\equiv P_{((g-i+1)p-(g-j+1))/g-(p-1)/(2g)}(\rho) \equiv w_{g-i+1,g-j+1} \pmod p.$$

2) If j is fixed and $\gcd(p, g) = 1$, then the congruence $ip - j \equiv (p-1)/2 \pmod g$ has only one solution for i and since $1 \leqslant i \leqslant g$, there is only one j. Therefore, in every row, only one non-zero element is possible. Similarly, we can show that in every column, there can be only one non-zero element. From this, it follows that W is a monomial matrix.

3,4) See Theorem 2. ■

It's known that the set of centrosymmetric matrices and the set of monomial matrices are closed under multiplication of matrices. Note that if W is centrosymmetric (monomial), then $W^{(p^k)}$ is also centrosymmetric (monomial). Therefore matrix W_p is centrosymmetric (monomial), if W is centrosymmetric (monomial).

For centrosymmetric matrices, there is an orthogonal transformation [19], which transforms such matrices to block-diagonal form. If the size of a centrosymmetric matrix is even, than this transformation is defined by the non-singular orthogonal matrix

$$Q = \sqrt{\frac{1}{2}} \begin{pmatrix} I & -J \\ J & I \end{pmatrix}.$$

And for odd case

$$Q = \sqrt{\frac{1}{2}} \begin{pmatrix} I & 0 & -J \\ 0 & \sqrt{2} & 0 \\ J & 0 & I \end{pmatrix}.$$

Note that this transformation is defined over $\mathbb{F}_q[\sqrt{2}]$ and a different transformation is required for Cartier — Manin matrices. The Cartier — Manin matrix W of any hyperelliptic curve is determined up to transformation of the form $S^{(p)}WS^{-1}$, where S is a non-singular matrix [20, Proposition 2.2]. The following theorem shows that, by modifying transformation for centrosymmetric matrices, we can choose S in such way that the resulting matrix is block-diagonal and defined over $\mathbb{F}_q$.

Theorem 5. Let $C_{1,\rho}$ be a genus g hyperelliptic curve, defined by equation $y^2 = x^{2g+1} - 2\rho x^{g+1} + x$ over the finite field $\mathbb{F}_q$, $\operatorname{char}\mathbb{F}_q = p > 2$. Then the Cartier — Manin matrix W of $C_{1,\rho}$ is equivalent to a block-diagonal matrix.

Proof. Let $W = \begin{pmatrix} W_1 & W_3 \\ W_2 & W_4 \end{pmatrix}$ if g is even, and $W = \begin{pmatrix} W_1 & a & W_3 \\ b & c & d \\ W_2 & e & W_4 \end{pmatrix}$ if g is odd. Since, by Theorem 4, the matrix W is centrosymmetric in $\mathbb{F}_q$, then W can be written in the form $W = \begin{pmatrix} W_1 & JW_2J \\ W_2 & JW_1J \end{pmatrix}$ for even g and $W = \begin{pmatrix} W_1 & a & JW_2J \\ b & c & bJ \\ W_3 & Ja & JW_1J \end{pmatrix}$ if g is odd.

Consider the transformation of the form $S^{(p)}WS^{-1}$.

1. If $\sqrt{2} \in \mathbb{F}_q$, then we choose $S = Q$ and have $S^{(p)}WS^{-1} = Q^{(p)}WQ^{\mathrm{T}}$. We need to show that this transformation transforms matrix to the block-diagonal form.

If genus g is even, then $Q^{(p)} = \left(\frac{1}{2}\right)^{(p-1)/2} Q$ and

$$Q^{(p)}WQ^{\mathrm{T}} = \left(\frac{1}{2}\right)^{(p-1)/2} \begin{pmatrix} W_1 - JW_2 & 0 \\ 0 & J(W_1 + JW_2)J \end{pmatrix}.$$

If genus g is odd, then $Q^{(p)}WQ^{\mathrm{T}} = \left(\frac{1}{2}\right)^{(p-1)/2} \begin{pmatrix} W_1 - JW_2 & 0 & 0 \\ 0 & 2^{(p-1)/2}c & \sqrt{2}^p b \\ 0 & \sqrt{2}Ja & J(W_1 + JW_2)J \end{pmatrix}$.

2. Let $\sqrt{2} \notin \mathbb{F}_q$, choose $S = \begin{pmatrix} I & 0 & -J \\ 0 & 1 & 0 \\ J & 0 & I \end{pmatrix}$ for odd g and $S = \begin{pmatrix} I & -J \\ J & I \end{pmatrix}$ for even g.

Then we have $S^{(p)} = S$, since $p > 2$, and $S^{-1} = \frac{1}{2}\begin{pmatrix} I & 0 & J \\ 0 & 2 & 0 \\ -J & 0 & I \end{pmatrix}$ or $S^{-1} = \frac{1}{2}\begin{pmatrix} I & J \\ -J & I \end{pmatrix}$.

Now, we have

$$S^{(p)}WS^{-1} = \begin{pmatrix} W_1 - JW_2 & 0 & 0 \\ 0 & c & bJ \\ 0 & 2Ja & J(W_1 + JW_2)J \end{pmatrix}$$

for odd case and

$$S^{(p)}WS^{-1} = \begin{pmatrix} W_1 - JW_2 & 0 \\ 0 & J(W_1 + JW_2)J \end{pmatrix}$$

for even case.

Note that in this case the matrix S is not orthogonal. If the orthogonality of S is not required, this transformation can also be applied to the case $\sqrt{2} \in \mathbb{F}_q$. ■

Applying this transformation to W_p, we get a formula for the characteristic polynomial of the matrix W_p and therefore for $\chi_q(\lambda)$.

Corollary 1. Let $C_{1,\rho} : y^2 = x^{2g+1} - 2\rho x^{g+1} + x$ be a genus g hyperelliptic curve over the field $\mathbb{F}_q$, $q = p^n$, $p > 2$ and the matrix W be written in the above form. Then

1) if g is even,

$$\chi_q(\lambda) \equiv (-1)^g \lambda^g |(W_1 + JW_2)_p - \lambda I||(W_1 - JW_2)_p - \lambda I| \pmod{p};$$

2) if g is odd and $p|g$,

$$\chi_q(\lambda) \equiv (-1)^g \lambda^g \left| \begin{pmatrix} P_{(p-1)/2}(\rho) & bJ \\ 2Ja & J(W_1 + JW_2)J \end{pmatrix}_p - \lambda I \right| |(W_1 - JW_2)_p - \lambda I| \pmod{p};$$

3) if g is odd and $p \nmid g$,

$$\chi_q(\lambda) \equiv (-1)^g \lambda^g (N_{F_q/F_p}(P_{(p-1)/2}(\rho)) - \lambda)|(W_1 + JW_2)_p - \lambda I||(W_1 - JW_2)_p - \lambda I| \pmod{p}.$$

If the matrix W is monomial, we can go further.

Theorem 6. Let W be the Cartier — Manin matrix of the curve $C_{1,\rho}$ over the finite field $\mathbb{F}_q$, $\gcd(p, g) = 1$; σ be a permutation such that $\sigma(i) \equiv ip - (p-1)/2 \pmod{g}$, and $P(\sigma)$ be the permutation matrix for σ. Then

1) if g is even,

$$W = \operatorname{diag}(w_{1,\sigma(1)}, \ldots, w_{g/2,\sigma(g/2)}, w_{g/2+1,g/2+1-\sigma(g/2)}, w_{g/2+2,g/2+1-\sigma(g/2-1)}, \ldots, w_{g,g+1-\sigma(1)})P(\sigma);$$

2) if g is odd,

$$W = \operatorname{diag}(w_{1,\sigma(1)}, \ldots, w_{(g-1)/2,\sigma((g-1)/2)}, w_{(g+1)/2,(g+1)/2}, w_{(g+1)/2+1,g+1-\sigma((g+1)/2-1)}, \ldots, w_{g,g+1-\sigma(1)})P(\sigma).$$

Proof. If $\gcd(p, g) = 1$, then W is a monomial matrix, which can be factored in the product of diagonal and permutation matrix: $W = \operatorname{diag}(w_{1,\sigma(1)}, \ldots, w_{g,\sigma(g)})P(\sigma)$. By Lemma 1, for non-zero elements of W, we have $ip - j \equiv (p-1)/2 \pmod{g}$. So the permutation σ is defined as $\sigma(i) \equiv ip - (p-1)/2 \pmod{g}$. Since the matrix $P(\sigma)$ is also centrosymmetric, every i such that $\sigma(i) \equiv ip - (p-1)/2 \pmod{g}$ uniquely determines the value of $\sigma(g+1-i)$, as $\sigma(g+1-i) \equiv g+1-\sigma(i) \pmod{g}$. ■

If we know the decomposition of σ^n into disjoint cycles, we can factor the polynomial $\chi_q(\lambda)$ in the following way.

Theorem 7. Let $C_{1,\rho} : y^2 = x^{2g+1} - 2\rho x^{g+1} + x$ be a hyperelliptic curve over the finite field $\mathbb{F}_q$, $q = p^n$, $\gcd(p, g) = 1$ and W be the Cartier — Manin matrix of this curve. Then W is the monomial matrix with the permutation σ such that $\sigma(i) \equiv ip - (p-1)/2 \pmod g$ and W_p is a monomial matrix with the permutation σ^n such that $\sigma^n(i) \equiv ip^n(p^n-1)/2 \pmod g$. If $W_p = (w'_{i,j})$ and $\sigma^n = \sigma_1\sigma_2 \dots \sigma_m$ is the decomposition of σ^n into disjoint cycles, then

$$\chi_q(\lambda) \equiv \lambda^g \prod_{j=1}^{m} (\lambda^{|\sigma_j|} - \prod_{k=1}^{|\sigma_j|} w'_{\sigma_{j,k},\sigma_{j,k+1}}) \pmod p,$$

where $\sigma_{j,k} = j_k$ for $\sigma_j = (j_1, \dots, j_{|\sigma_j|})$.

Proof. If W is the monomial matrix with the permutation σ, then, by multiplying matrices, we obtain

$$W_p = (w'_{i,j}) = \left(w^{p^{n-1}}_{\sigma^{n-1}(i),j} \prod_{k=0}^{n-2} w^{p^k}_{\sigma^k(i),\sigma^{k+1}(i)} \right),$$

where σ^k are permutations with $\sigma^k(i) \equiv ip^k - (p^k-1)/2 \pmod g$ and $w'_{i,j} = 0$ for all $j \neq \neq \sigma^n(i)$. Therefore, W_p is a monomial matrix with the permutation $\sigma^n(i) \equiv ip^n - (p^n-1)/2 \pmod g$ and the result follows from the Theorem 1. ■

In the case of the diagonal matrix, the formula can be made simpler.

Theorem 8. Let $C_{1,\rho} : y^2 = x^{2g+1} - 2\rho x^{g+1} + x$ be a genus g hyperelliptic curve over the finite field $\mathbb{F}_q$, $q = p^n$, $p > 2$. Then

1) if g is even and $p \equiv 1 \pmod{2g}$,

$$\chi_q(\lambda) \equiv \lambda^g \prod_{i=1}^{g/2} (\lambda - N_{\mathbb{F}_q/\mathbb{F}_p}(P_{(2i-1)(p-1)/(2g)}(\rho)))^2 \pmod p;$$

2) if g is odd and $p \equiv 1 \pmod g$,

$$\chi_q(\lambda) \equiv \lambda^g (\lambda - N_{\mathbb{F}_q/\mathbb{F}_p}(P_{(p-1)/2}(\rho))) \prod_{i=1}^{(g-1)/2} (\lambda - N_{\mathbb{F}_q/\mathbb{F}_p}(P_{(2i-1)(p-1)/(2g)}(\rho)))^2 \pmod p.$$

2.2. Curves of the form $y^2 = x^{2g+2} + ax^{g+1} + b$

The following curves of this form

$$C_2 : y^2 = x^{2g+2} + ax^{g+1} + b,$$
$$C_{2,\rho} : y^2 = x^{2g+2} - 2\rho x^{g+1} + 1$$

have the properties similar to the curves C_1 and $C_{1,\rho}$. We collect them in the following theorem.

Theorem 9. Let $C_{2,\rho}$ be a hyperelliptic curve defined by the equation $y^2 = x^{2g+2} - \\ - 2\rho x^{g+1} + 1$ over finite field $\mathbb{F}_q$ and $W = (w_{i,j})$ be the Cartier — Manin matrix of $C_{2,\rho}$. Then

1) $w_{i,j} = 0$ if $ip \not\equiv j \pmod{g+1}$;
2) $w_{i,j} \equiv P_{(ip-j)/(g+1)}(\rho) \pmod{g+1}$;
3) W is a centrosymmetric matrix in $\mathbb{F}_q$;
4) W is a monomial matrix if $p \nmid (g+1)$;
5) W is a diagonal matrix if $p \nmid (g+1)$ and $p \equiv 1 \pmod{g+1}$;

6) W is an anti-diagonal matrix if $p \nmid (g+1)$ and $p \equiv -1 \pmod{g+1}$;
7) there is a transformation of the form $S^{(p)} W S^{-1}$ where S is non-singular, which transforms W to a block-diagonal form;
8) if g is even,

$$\chi_q(\lambda) \equiv (-1)^g \lambda^g |(W_1 + JW_2)_p - \lambda I||(W_1 - JW_2)_p - \lambda I| \pmod{p};$$

9) if g is odd and $p|g$,

$$\chi_q(\lambda) \equiv (-1)^g \lambda^g \left| \begin{pmatrix} P_{(p-1)/2}(\rho) & bJ \\ 2Ja & J(W_1 + JW_2)J \end{pmatrix}_p - \lambda I \right| |(W_1 - JW_2)_p - \lambda I| \pmod{p};$$

10) if g is odd and $p \nmid g$,

$$\chi_q(\lambda) \equiv (-1)^g \lambda^g (N_{F_q/F_p}(P_{(p-1)/2}(\rho)) - \lambda) |(W_1 + JW_2)_p - \lambda I||(W_1 - JW_2)_p - \lambda I| \pmod{p}.$$

Proof.
1) It follows from Lemma 1.
2) Let $(g+1)|(ip-j)$ and $t = x^{g+1}$. Then

$$w_{i,j} = [x^{ip-j}](x^{2g+2} - 2\rho x^{g+1} + 1)^{(p-1)/2} = [t^{(ip-j)/(g+1)}](t^2 - 2\rho t + 1)^{(p-1)/2} \equiv P_{(ip-j)/(g+1)}(\rho) \pmod{p}.$$

3) $w_{i,j} \equiv P_{(ip-j)/(g+1)} \equiv P_{p-1-(ip-j)/(g+1)} \equiv w_{g+1-i,g+1-j}$.
4) If $\gcd(p, g+1) = 1$, then the congruence $ip \equiv j \pmod{g+1}$ has only one solution for each i, j, and since $1 \leqslant i, j \leqslant g$ it uniquely determines i, j.
5, 6) These follow from congruences $i \equiv j \pmod{g+1}$ and $i \equiv -j \pmod{g+1}$ for $1 \leqslant i, j \leqslant g$.
7–10) The needed transformations are taken from the Theorem 5. ■

Conclusion

We have proved that the Cartier — Manin matrices W for the curves $C_{1,\rho}$ and $C_{2,\rho}$ have a very special form, namely, the coefficients of W are the Legendre polynomials, W is centrosymmetric and is equivalent to a block-diagonal matrix. In the case $\gcd(p, g) = 1$, the matrices of C_1 and C_2 are monomial. Using this fact, we have proved (Theorem 7) that the polynomial $\chi_q(\lambda)$ modulo p can be computed in a factored form in terms of the Legendre polynomials. The matrix symmetry can be used to speed up the algorithms for computing the Cartier — Manin matrices, because it is enough to compute half of coefficients to completely determine a matrix itself. As an application, we have listed all the possible variants of the polynomial $\chi_p(\lambda)$ modulo p for the curve C_1 over prime field (Table 1) and over $\mathbb{F}_{p^2}$ (Table 2).

T a b l e 1

Hyperelliptic curves of the form $C_{1,\rho} : y^2 = x^{2g+1} + ax^{g+1} + bx$ over the prime field $\mathbb{F}_p$, $p > 2$, $p \nmid g$, $P_m := P_m(\rho)$ and b is a square

g	Conditions	$\chi_p(\lambda) \pmod{p}$
2	$p \equiv 1 \pmod 4$	$\lambda^2(\lambda - P_{(p-1)/4})^2$
2	$p \equiv 3 \pmod 4$	$\lambda^2(\lambda^2 - P^2_{(p-3)/4})$
3	$p \equiv 1 \pmod 3$	$\lambda^3(\lambda - P_{(p-1)/2})(\lambda - P_{(p-1)/6})^2$
3	$p \equiv 2 \pmod 3$	$\lambda^3(\lambda - P_{(p-1)/2})(\lambda^2 - P^2_{(p-5)/6})$
4	$p \equiv 1 \pmod 8$	$\lambda^4(\lambda - P_{(p-1)/8})^2(\lambda - P_{(3p-3)/8})^2$
4	$p \equiv 3 \pmod 8$	$\lambda^4(\lambda^2 - P_{(p-3)/8}P_{(3p-1)/8})^2$

End of Table 1

g	Conditions	$\chi_p(\lambda) \pmod p$
4	$p \equiv 5 \pmod 8$	$\lambda^4(\lambda^2 - P_{(p-5)/8}P_{(3p-7)/8})^2$
4	$p \equiv 7 \pmod 8$	$\lambda^4(\lambda^2 - P^2_{(p-7)/8})(\lambda^2 - P^2_{(3p-5)/8})$
5	$p \equiv 1 \pmod 5$	$\lambda^5(\lambda - P_{(p-1)/2})(\lambda - P_{(p-1)/10})^2(\lambda - P_{(3p-3)/10})^2$
5	$p \equiv 2 \pmod 5$	$\lambda^5(\lambda - P_{(p-1)/2})(\lambda^4 - P^2_{(p-7)/10}P^2_{(3p-1)/10})$
5	$p \equiv 3 \pmod 5$	$\lambda^5(\lambda - P_{(p-1)/2})(\lambda^4 - P^2_{(p-3)/10}P^2_{(3p-9)/10})$
5	$p \equiv 4 \pmod 5$	$\lambda^5(\lambda - P_{(p-1)/2})(\lambda^2 - P^2_{(p-9)/10})(\lambda^2 - P^2_{(3p-7)/10})$
6	$p \equiv 1 \pmod{12}$	$\lambda^6(\lambda - P_{(p-1)/12})^2(\lambda - P_{(p-1)/4})^2(\lambda - P_{(5p-5)/12})^2$
6	$p \equiv 5 \pmod{12}$	$\lambda^6(\lambda - P_{(p-1)/4})^2(\lambda^2 - P_{(p-5)/12}P_{(5p-1)/12})^2$
6	$p \equiv 7 \pmod{12}$	$\lambda^6(\lambda^2 - P_{(p-7)/12}P_{(5p-11)/12})^2(\lambda^2 - P^2_{(p-3)/4})$
6	$p \equiv 11 \pmod{12}$	$\lambda^6(\lambda^2 - P^2_{(p-11)/12})(\lambda^2 - P^2_{(p-3)/4})(\lambda^2 - P^2_{(5p-7)/12})$
7	$p \equiv 1 \pmod 7$	$\lambda^7(\lambda - P_{(p-1)/2})(\lambda - P_{(p-1)/14})^2(\lambda - P_{(3p-3)/14})^2(\lambda - P_{(5p-5)/14})^2$
7	$p \equiv 2 \pmod 7$	$\lambda^7(\lambda - P_{(p-1)/2})(\lambda^3 - P_{(p-9)/14}P_{(3p-13)/14}P_{(5p-3)/14})^2$
7	$p \equiv 3 \pmod 7$	$\lambda^7(\lambda - P_{(p-1)/2})(\lambda^6 - P^2_{(p-3)/14}P^2_{(3p-9)/14}P^2_{(5p-1)/14})$
7	$p \equiv 4 \pmod 7$	$\lambda^7(\lambda - P_{(p-1)/2})(\lambda^3 - P_{(p-11)/14}P_{(3p-5)/14}P_{(5p-13)/14})^2$
7	$p \equiv 5 \pmod 7$	$\lambda^7(\lambda - P_{(p-1)/2})(\lambda^6 - P^2_{(5p-11)/14}P^2_{(3p-1)/14}P^2_{(p-5)/14})$
7	$p \equiv 6 \pmod 7$	$\lambda^7(\lambda - P_{(p-1)/2})(\lambda^2 - P^2_{(p-13)/14})(\lambda^2 - P^2_{(3p-11)/14})(\lambda^2 - P^2_{(5p-9)/14})$

Table 2

Hyperelliptic curves of the form $C_{1,\rho} : y^2 = x^{2g+1} + ax^{g+1} + bx$ over the field $\mathbb{F}_{p^2}$, $p > 2$, $p \nmid g$, $P_m := P_m(\rho)$, b is a square in $\mathbb{F}_{p^2}$

g	Conditions	$\chi_{p^2}(\lambda) \pmod p$
2	$p \equiv 1 \pmod 4$	$\lambda^2(\lambda - P^{p+1}_{(p-1)/4})^2$
2	$p \equiv 3 \pmod 4$	$\lambda^2(\lambda - P^{p+1}_{(p-3)/4})^2$
3	$p \equiv 1 \pmod 3$	$\lambda^3(\lambda - P^{p+1}_{(p-1)/2})(\lambda - P^{p+1}_{(p-1)/6})^2$
3	$p \equiv 2 \pmod 3$	$\lambda^3(\lambda - P^{p+1}_{(p-1)/2})(\lambda - P^{p+1}_{(p-5)/6})^2$
4	$p \equiv 1 \pmod 8$	$\lambda^4(\lambda - P^{p+1}_{(p-1)/8})^2(\lambda - P^{p+1}_{(3p-3)/8})^2$
4	$p \equiv 3 \pmod 8$	$\lambda^4(\lambda - P^{p}_{(p-3)/8}P_{(3p-1)/8})^2(\lambda - P^{p}_{(3p-1)/8}P_{(p-3)/8})^2$
4	$p \equiv 5 \pmod 8$	$\lambda^4(\lambda - P^{p}_{(p-5)/8}P_{(3p-7)/8})^2(\lambda - P^{p}_{(3p-7)/8}P_{(p-5)/8})^2$
4	$p \equiv 7 \pmod 8$	$\lambda^4(\lambda - P^{p+1}_{(p-7)/8})^2(\lambda - P^{p+1}_{(3p-5)/8})^2$
5	$p \equiv 1 \pmod 5$	$\lambda^5(\lambda - P^{p+1}_{(p-1)/2})(\lambda - P^{p+1}_{(p-1)/10})^2(\lambda - P^{p+1}_{(3p-3)/10})^2$
5	$p \equiv 2 \pmod 5$	$\lambda^5(\lambda^2 - P^{2p}_{(p-7)/10}P^2_{(3p-1)/10})(\lambda^2 - P^{2p}_{(3p-1)/10}P^2_{(p-7)/10})(\lambda - P^{p+1}_{(p-1)/2})$
5	$p \equiv 3 \pmod 5$	$\lambda^5(\lambda^2 - P^{2p}_{(p-3)/10}P^2_{(3p-9)/10})(\lambda^2 - P^{2p}_{(3p-9)/10}P^2_{(p-3)/10})(\lambda - P^{p+1}_{(p-1)/2})$
5	$p \equiv 4 \pmod 5$	$\lambda^5(\lambda - P^{p+1}_{(p-1)/2})(\lambda - P^{p+1}_{(p-9)/10})^2(\lambda - P^{p+1}_{(3p-7)/10})^2$
6	$p \equiv 1 \pmod{12}$	$\lambda^6(\lambda - P^{p+1}_{(p-1)/4})^2(\lambda - P^{p+1}_{(p-1)/12})^2(\lambda - P^{p+1}_{(5p-5)/12})^2$
6	$p \equiv 5 \pmod{12}$	$\lambda^6(\lambda - P^{p}_{(p-5)/12}P_{(5p-1)/12})^2(\lambda - P^{p}_{(5p-1)/12}P_{(p-5)/12})^2(\lambda - P^{p+1}_{(p-1)/4})^2$
6	$p \equiv 7 \pmod{12}$	$\lambda^6(\lambda - P^{p}_{(p-7)/12}P_{(5p-11)/12})^2(\lambda - P^{p}_{(5p-11)/12}P_{(p-7)/12})^2(\lambda - P^{p+1}_{(p-3)/4})^2$
6	$p \equiv 11 \pmod{12}$	$\lambda^6(\lambda - P^{p+1}_{(p-3)/4})^2(\lambda - P^{p+1}_{(p-11)/12})^2(\lambda - P^{p+1}_{(5p-7)/12})^2$
7	$p \equiv 1 \pmod 7$	$\lambda^7(\lambda - P^{p+1}_{(p-1)/2})(\lambda - P^{p+1}_{(p-1)/14})^2(\lambda - P^{p+1}_{(5p-5)/14})^2(\lambda - P^{p+1}_{(3p-3)/14})^2$
7	$p \equiv 2 \pmod 7$	$\lambda^7(\lambda - P^{p+1}_{(p-1)/2})(\lambda^3 - P^{p+1}_{(p-9)/14}P^{p+1}_{(5p-3)/14}P^{p+1}_{(3p-13)/14})^2$
7	$p \equiv 3 \pmod 7$	$\lambda^7(\lambda - P^{p+1}_{(p-1)/2})(\lambda^3 - P^{p+1}_{(p-3)/14}P^{p+1}_{(3p-9)/14}P^{p+1}_{(5p-1)/14})^2$
7	$p \equiv 4 \pmod 7$	$\lambda^7(\lambda - P^{p+1}_{(p-1)/2})(\lambda^3 - P^{p+1}_{(p-11)/14}P^{p+1}_{(3p-5)/14}P^{p+1}_{(5p-13)/14})^2$
7	$p \equiv 5 \pmod 7$	$\lambda^7(\lambda^3 - P^{p+1}_{(p-5)/14}P^{p+1}_{(3p-1)/14}P^{p+1}_{(5p-11)/14})^2(\lambda - P^{p+1}_{(p-1)/2})$
7	$p \equiv 6 \pmod 7$	$\lambda^7(\lambda - P^{p+1}_{(p-1)/2})(\lambda - P^{p+1}_{(p-13)/14})^2(\lambda - P^{p+1}_{(3p-11)/14})^2(\lambda - P^{p+1}_{(5p-9)/14})^2$

Our results were checked in Pari/GP and Sage.

A short information about these results were presented by the author on the conference Sibecrypt'17 [21].

REFERENCES

1. *Koblitz N.* Hyperelliptic cryptosystems. J. Cryptology, 1989, vol. 1, no. 3, pp. 139–150.
2. *Enge A. and Gaudry P.* A general framework for subexponential discrete logarithm algorithms. Acta Arith., 2000, vol. 102, pp. 83–103.
3. *Enge A., Gaudry P., and Thomé E.* An $L(1/3)$ discrete logarithm algorithm for low degree curves. J. Cryptology, 2011, vol. 24, no. 1, pp. 24–41.
4. *Gaudry P., Thomé E., Thériault N., and Diem C.* A double large prime variation for small genus hyperelliptic index calculus. Math. Comput., 2007, vol. 76, no. 257, pp. 475–492.
5. *Barbulescu R., Gaudry P., Joux A., and Thomé E.* A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. LNCS, 2014, vol. 8441, pp. 1–16.
6. *Manin Yu. I.* O matritse Khasse — Vitta algebraicheskoy krivoy [The Hasse-Witt matrix of an algebraic curve]. Izv. Akad. Nauk SSSR, Ser. Mat., 1961, vol. 25, no. 1, pp. 153–172. (in Russian)
7. *Bostan A., Gaudry P., and Schost; E.* Linear recurrences with polynomial coefficients and application to integer factorization and Cartier — Manin operator. SIAM J. Comput., 2007, vol. 36, no. 6, pp. 1777–1806.
8. *Harvey D. and Sutherland A. V.* Hasse — Witt matrices of hyperelliptic curves in average polynomial time. LMS J. Comput. Math., 2014, vol. 17, no. A, pp. 257–273.
9. *Yui N.* Jacobi quartics, Legendre polynomials and formal groups. Lecture Notes in Mathematics, 1988, vol. 1326, pp. 182–215.
10. *Miller L.* The Hasse — Witt-matrix of special projective varieties. Pacific J. Math., 1972, vol. 43, no. 2, pp. 443–455.
11. *Miller L.* Curves with invertible Hasse — Witt-matrix. Math. Ann., 1972, vol. 197, pp. 123–127.
12. *Leprevost F. and Morain F.* Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères. J. Number Theory, 1997, vol. 64, no. 2, pp. 165–182.
13. *Brillhart J. and Morton P.* Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial. J. Number Theory, 2004, vol. 106, no. 1, pp. 79–111.
14. *Satoh T.* Generating genus two hyperelliptic curves over large characteristic finite fields. LNCS, 2009, vol. 5479, pp. 536–553.
15. *Freeman D. M. and Satoh T.* Constructing pairing-friendly hyperelliptic curves using Weil restriction. J. Number Theory, 2011, vol. 131, no. 5, pp. 959–983.
16. *Guillevic A. and Vergnaud D.* Genus 2 hyperelliptic curve families with explicit Jacobian order evaluation and pairing-friendly constructions. LNCS, 2012, vol. 7708, pp. 234–253.
17. *Garcia-Planas M. I. and Magret M. D.* Eigenvectors of permutation matrices. Adv. Pure Math., 2015, vol. 5, no. 7, pp. 390–393.
18. *Carlitz L.* Congruence properties of the polynomials of Hermite, Laguerre and Legendre. Mathematische Zeitschrift, 1953, vol. 59, pp. 474–483.
19. *Weaver J. R.* Centrosymmetric (cross-symmetric) matrices, their basic properties, eigenvalues, and eigenvectors. Amer. Math. Monthly, 1985, vol. 92, no. 10, pp. 711–717.
20. *Yui N.* On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$. J. Algebra, 1978, vol. 52, no. 2, pp. 378–410.
21. *Novoselov S. A.* Hyperelliptic curves, Cartier — Manin matrices and Legendre polynomials. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2017, no. 10, pp. 30–32.