Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2011, Article ID 437541, 25 pages
doi:10.1155/2011/437541

Research Article

Computing the Characteristic Polynomials of a Class of Hyperelliptic Curves for Cryptographic Applications

Lin You,[1, 2] Guangguo Han,[1] Jiwen Zeng,[3] and Yongxuan Sang[1]

[1] *College of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China*
[2] *College of Engineering and Science, Clemson University, Clemson, SC 29631, USA*
[3] *School of Mathematical Sciences, Xiamen University, Xiamen 361005, China*

Correspondence should be addressed to Lin You, lyou@g.clemson.edu

Received 12 November 2010; Accepted 21 March 2011

Academic Editor: J. Rodellar

Hyperelliptic curves have been widely studied for cryptographic applications, and some special hyperelliptic curves are often considered to be used in practical cryptosystems. Computing Jacobian group orders is an important operation in constructing hyperelliptic curve cryptosystems, and the most common method used for the computation of Jacobian group orders is by computing the zeta functions or the characteristic polynomials of the related hyperelliptic curves. For the hyperelliptic curve C_q: $v^2 = u^p + au + b$ over the field $\mathbb{F}_q$ with q being a power of an odd prime p, Duursma and Sakurai obtained its characteristic polynomial for $q = p$, $a = -1$, and $b \in \mathbb{F}_p$. In this paper, we determine the characteristic polynomials of C_q over the finite field $\mathbb{F}_{p^n}$ for $n = 1$, 2 and $a, b \in \mathrm{F}_{p^n}$. We also give some computational data which show that many of those curves have large prime factors in their Jacobian group orders, which are both practical and vital for the constructions of efficient and secure hyperelliptic curve cryptosystems.

1. Introduction and Main Results

1.1. Hyperelliptic Curves and Cryptosystems

A hyperelliptic curve C of genus g over $\mathbb{F}_q$ is defined by an equation of the form

$$v^2 + h(u)v = f(u), \tag{1.1}$$

where $h(u)$, $f(u) \in \mathbb{F}_q[u]$ with $\deg_u(h) \leq g$ and $\deg_u(f) = 2g + 1$, and the equation system $v^2 + h(u)v = f(u)$, $2v + h(u) = 0$, and $h'(u)v - f'(u) = 0$ has no solutions in $\overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$.

For an extension $\mathbb{K}$ of $\mathbb{F}_q$, the set

$$C(\mathbb{K}) = \left\{ (x, y) \in \mathbb{K} \times \mathbb{K} \mid y^2 + h(x)\ y = f(x) \right\} \cup \{\infty\} \tag{1.2}$$

is called the set of $\mathbb{K}$-rational points on C. The symbol ∞ is called the point at infinity, and the other points are called finite points.

A *divisor D* is defined as a finite formal sum of finite points or the infinity ∞, while the *Jacobian group* (or simply called *Jacobian*) of the curve C over $\mathbb{K}$ is an Abelian group composed of some special divisors (i.e., reduced divisors) on C. This Jacobian group is generally denoted as $\mathbb{J}_C(\mathbb{K})$. A hyperelliptic curve cryptosystem (HECC) is a cryptosystem constructed on the Jacobian group of the hyperelliptic curve over a finite field. For example, the hyperelliptic curve digital signature algorithm (HECDSA) is a hyperelliptic curve version of an elliptic curve digital signature algorithm (ECDSA). The security of an HECC is based on the discrete logarithm problems in the corresponding Jacobian group.

Since HECC was invented by Koblitz [1] in 1989, it has been extensively researched, and now it has been considered for practical cryptographic applications. For a certain number of classes of hyperelliptic curves with some specific parameters, the corresponding HECC can even possess lower complexities than an elliptic curve cryptosystem but with the same level of security [2].

In order to construct a secure HECC, one first has to choose a hyperelliptic curve over a finite field and then compute the order of the hyperelliptic curve Jacobian group. If the order does not have a large prime factor, then the discrete logarithm problems in this Jacobian group may not be hard enough to guarantee the security of the HECC, and so the hyperelliptic curve is not suitable for cryptographic uses and should be chosen again to ensure that the Jacobian group order has some large prime factor. But, in most cases, this computation is a very time-consuming task. Hence, the computation of Jacobian group order is a very important step for the efficient implementation of HECC.

1.2. Zeta Functions and Jacobian Group Orders

The most common method used for the computation of Jacobian group orders is by computing the numerator of the zeta functions of the related hyperelliptic curves, or by computing the characteristic polynomial of the hyperelliptic curve. The following results are due to the Weil's theorem [3, 4] and Kedlaya's algorithm [5].

Let C be a hyperelliptic curve of (1.1) over $\mathbb{F}_q$. For any positive integer r, let N_r denote the number of $\mathbb{F}_{q^r}$-rational points on C. The zeta function of C is defined as

$$Z(t) = Z(C; t) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r} \right). \tag{1.3}$$

Then

(a) $Z(t)$ is a rational function over $\mathbb{Z}$ and can be written as $Q(t)/(1-t)(1-qt)$, where $Q(t) \in \mathbb{Z}[t]$,

(b) there exist complex numbers τ_i $(i = 1, \ldots, 2g)$ with $|\tau_i| = \sqrt{q}$ such that

$$Q(t) = \prod_{i=1}^{2g}(1 - \tau_i t), \qquad N_r = q^r + 1 - \sum_{i=1}^{2g}\tau_i^r, \tag{1.4}$$

(c) the integer coefficient polynomial

$$P(t) = t^{2g}Q\left(\frac{1}{t}\right) = \prod_{i=1}^{2g}(t - \tau_i) \tag{1.5}$$

is called the characteristic polynomial of the Frobenius endomorphism on $\mathbb{J}_C(\mathbb{F}_q)$ (it is also called the characteristic polynomial of C over $\mathbb{F}_q$), and it is can be expressed as

$$P(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_g t^g + q a_{g-1} t^{g-1} + \cdots + q^{g-1} a_1 t + q^g, \tag{1.6}$$

where for $1 \leq i \leq$ g,

$$i a_i = \left(N_i - q^i - 1\right) + \left(N_{i-1} - q^{i-1} - 1\right)a_1 + \cdots + (N_1 - q - 1)a_{i-1}, \tag{1.7}$$

(d) for any positive integer n, the order of $\mathbb{J}_C(\mathbb{F}_{q^n})$ is given as

$$\#\mathbb{J}_C(\mathbb{F}_{q^n}) = \prod_{i=1}^{2g}(1 - \tau_i^n). \tag{1.8}$$

Hence, for any positive integer n, the order of $\mathbb{J}_C(\mathbb{F}_{q^n})$ can be computed if $P(t)$ is determined or if $N_r (1 \leq r \leq g)$ are computed.

For a positive integer j, the quadratic character χ_j of $\mathbb{F}_{q^j}$ is defined as

$$\chi_j : \alpha \longmapsto \begin{cases} 1 & \text{if } \alpha \text{ is a quadratic residue in } \mathbb{F}_{q^j}, \\ 0 & \text{if } \alpha = 0, \\ -1 & \text{if } \alpha \text{ is a non-quadratic residue in } \mathbb{F}_{q^j}. \end{cases} \tag{1.9}$$

Obviously, $\chi_j(\alpha\beta) = \chi_j(\alpha)\chi_j(\beta)$ holds for any $\alpha, \beta \in \mathbb{F}_{q^j}$. By using χ_j, we can compute N_j as

$$\begin{aligned} N_j &= 1 + \left|\left\{(x, y) \in \mathbb{F}_{q^j} \times \mathbb{F}_{q^j} \mid y^2 = f(x)\right\}\right| \\ &= 1 + \sum_{x\in\mathbb{F}_{q^j}} \left(\chi_j(f(x)) + 1\right) \\ &= q^j + 1 + \sum_{x\in\mathbb{F}_{q^j}} \chi_j(f(x)). \end{aligned} \tag{1.10}$$

While for any positive integer j and every field element $\alpha \in \mathbb{F}_{q^j}$, the value of the extended quadratic character χ_j at α can be computed as $\chi_j(\alpha) = \alpha^{(q^j-1)/2}$ in $\mathbb{F}_q$.

1.3. Our Main Results

Let C_q be the curve with the equation

$$C_q : v^2 = u^p + au + b \quad \text{over } \mathbb{F}_q, \tag{1.11}$$

where $a \neq 0$ and q is a power of an odd prime p. Then C_q is a hyperelliptic curve of genus $(p-1)/2$. In [6], Duursma and Sakurai presented $Q(t)$ of C_q for $q = p$ and $a = -1$. That is, the numerator of the corresponding zeta function is given as

$$Q(t) = \prod_{k=1}^{p-1}\left(1 - \left(\frac{k}{p}\right)\zeta^k\sqrt{\tilde{p}}t\right) \quad \text{or} \quad \prod_{k=1}^{p-1}\left(1 + \left(\frac{k}{p}\right)\zeta^k\sqrt{\tilde{p}}t\right), \tag{1.12}$$

respectively, where $\tilde{p} = (-1/p)p$, $\sqrt{\tilde{p}} = -(-1/p)\sum_{k=1}^{p-1}(k/p)\zeta^k$, ζ is a p-th unity root, and (k/p) denotes the Legendre symbol.

In this paper, we compute the characteristic polynomials of C_q with $a, b \in \mathbb{F}_q$ $(q = p^n, n = 1, 2)$ and get the following Table 1.

From the characteristic polynomials of the hyperelliptic curve C_p over $\mathbb{F}_{p^n}$, the orders of Jacobian groups $\mathbb{J}_{C_p}(\mathbb{F}_{p^n})$ can be easily computed as

$$\#\mathbb{J}_{C_p}(\mathbb{F}_{p^n}) = \prod_{i=1}^{p-1}(1 - \tau_i^n). \tag{1.13}$$

For example, if a is a primitive element modulo p, then the characteristic polynomial of C_p is

$$P(t) = t^{p-1} + p^{(p-1)/2} = \prod_{\zeta^{p-1}=1}(t - \zeta\lambda\sqrt{p}), \tag{1.14}$$

Table 1: The characteristic polynomials of the curve $v^2 = u^p + au + b$ over $\mathbb{F}_{p^n}$.

n	a	b	$P(t)$ over $\mathbb{F}_{p^n}$	Notes
1	-1	$b = 0$	$(t^2 - \tilde{p})^{(p-1)/2}$	
	1	$b \in \mathbb{F}_p$	$(t^2 + p)^{(p-1)/2}$	
	a primitive root modulo p	$b \in \mathbb{F}_p$	$t^{p-1} + p^{(p-1)/2}$	
	$\mathrm{ord}_{\mathbb{F}_p^*}(a) = m$	$b \in \mathbb{F}_p$	$(t^m + (-1/p)(-p)^{m/2})^{(p-1)/m}$	m is even
	$2 < m < p - 1$		$(t^{2m} + p^m)^{(p-1)/2m}$	m is odd
2	-1	$b = 0$	$(t - \tilde{p})^{p-1}$	
		$b(\neq 0) \in \mathbb{F}_{p^2}$	$(t^p - \tilde{p}^p)/(t - \tilde{p})$	
	1	$b \in \mathbb{F}_p$	$(t + p)^{p-1}$	
		$b \notin \mathbb{F}_p$	$(t^p + p^p)/(t + p)$	
	a primitive root of p	$b \in \mathbb{F}_{p^2}$	$(t^{(p-1)/2} + p^{(p-1)/2})^2$	
	$\mathrm{ord}_{\mathbb{F}_p^*}(a) = m$	$b \in \mathbb{F}_{p^2}$	$(t^{m/2} + (-1/p)(-p)^{m/2})^{2(p-1)/m}$	m is even
	$2 < m < p - 1$		$(t^m + p^m)^{(p-1)/m}$	m is odd
	$a \notin \mathbb{F}_p$, $m = \mathrm{ord}_{\mathbb{F}_{p^2}^*}(a)$	$b \in \mathbb{F}_{p^2}$	$(t^e + (-1)^{e(p+1)/m+e-1} p^e)^{(p-1)/e}$	$e(> 1)$ is the smallest s.t. $m \mid e(p + 1)$.
	$a \notin \mathbb{F}_p$, $a^{p+1} = 1$	$b = 0$, or $a = b^{1-p}$	$(t + a^{(p+1)/2} p)^{p-1}$	
		$b \neq 0$, $a \neq b^{1-p}$	$(t^p + p^p)/(t + p)$	

where λ satisfies $\lambda^{p-1} + 1 = 0$. Hence, the order of the Jacobian group of C_p over $\mathbb{F}_{p^n}$ is

$$\#\mathbb{J}_{C_p}(\mathbb{F}_{p^n}) = \prod_{\zeta^{p-1}=1} \left(1 - (\zeta\lambda\sqrt{p})^n\right). \tag{1.15}$$

If n is an integer coprime to $p-1$, let $\eta = \zeta^n$; then η will also run through all these roots when ζ runs through the all roots of $x^{p-1} - 1 = 0$. Hence, we have

$$\begin{aligned} \prod_{\zeta^{p-1}=1} \left(1 - (\zeta\lambda\sqrt{p})^n\right) &= \prod_{\zeta^{p-1}=1} \left(1 - \zeta^n (\lambda\sqrt{p})^n\right) = \prod_{\eta^{p-1}=1} \left(1 - \eta(\lambda\sqrt{p})^n\right) = 1 - \left((\lambda\sqrt{p})^n\right)^{p-1} \\ &= 1 - \left(\lambda^{\mathrm{p}-1}\right)^n \left((\sqrt{p})^n\right)^{p-1} = 1 - (-1)^n \left(\sqrt{p}\right)^{n(p-1)} = 1 + \sqrt{p}^{n(p-1)}. \end{aligned} \tag{1.16}$$

If n is an integer not coprime to $p-1$, let d be the factor of n such that $\gcd(n/d, p-1) = 1$, then we have

$$\begin{aligned} \prod_{\zeta^{p-1}=1} \left(1 - (\zeta\lambda\sqrt{p})^n\right) &= \prod_{\zeta^{p-1}=1} \left(1 - \left((\zeta\lambda\sqrt{p})^{n/d}\right)^d\right) = \prod_{\zeta^{p-1}=1} \left(\prod_{\xi^d=1} \left(1 - \xi(\zeta\lambda\sqrt{p})^{n/d}\right)\right) \\ &= \prod_{\xi^d=1} \left(\prod_{\zeta^{p-1}=1} \left(1 - \xi(\zeta\lambda\sqrt{p})^{n/d}\right)\right) = \prod_{\xi^d=1} \left(\prod_{\zeta^{p-1}=1} \left(1 - \zeta^{n/d} \left(\xi^{d/n} \lambda\sqrt{p}\right)^{n/d}\right)\right) \end{aligned}$$

$$\begin{aligned}
&= \prod_{\xi^d=1}\left(1-\left(\left(\xi^{d/n}\lambda\sqrt{p}\right)^{n/d}\right)^{p-1}\right) = \prod_{\xi^d=1}\left(1-\xi^{p-1}\lambda^{n(p-1)/d}\sqrt{p}^{n(p-1)/d}\right) \\
&= \prod_{\xi^d=1}\left(1-\lambda^{n(p-1)/d}\sqrt{p}^{n(p-1)/d}\right) = \left(1-(-1)^{n/d}\sqrt{p}^{n(p-1)/d}\right)^{d}.
\end{aligned} \tag{1.17}$$

That is, for any positive integer n, the order of the Jacobian group of the curve C_p over $\mathbb{F}_{p^n}$ with a being a primitive element modulo p can be computed as

$$\#\mathbb{J}_{C_p}(\mathbb{F}_{p^n}) = \left(1-(-1)^{n/d}\sqrt{p}^{n(p-1)/d}\right)^{d}, \tag{1.18}$$

where d is the factor of n such that $\gcd(n/d, p-1) = 1$.

In Table 2, we give some essential parameters with which the Jacobian group order of C_q has some large prime factors, which shows that the C_q with these parameters may be used for cryptographic applications.

2. Isomorphic Curves, Twisted Curves, and Their Characteristic Polynomials

Two hyperelliptic curves of the same genus over the field $\mathbb{F}$ are called isomorphic over $\mathbb{F}$ if they are isomorphic as projective varieties over $\mathbb{F}$. If C_1 and C_2 are isomorphic over $\mathbb{F}$, then their Jacobian groups $\mathbb{J}_{C_1}(\mathbb{F})$ and $\mathbb{J}_{C_2}(\mathbb{F})$ are also isomorphic [7]. Hence, the hyperelliptic curve cryptosystem based on the Jacobian group of C_1 is equivalent to that based on the Jacobian group of C_2.

From [8], we know how to the hyperelliptic curves are isomorphic. Precisely, suppose C_1 and C_2 are two hyperelliptic curves of the equation forms $H_i :\ v^2+h_i(u)v = f_i(u)\ (i = 1,2)$, respectively, with $h_i(u)$, $f_i(u)$ (monic) $\in \mathbb{F}[u]$, $\deg(h_i(u)) \le g$, and $\deg(f_i(u)) = 2g+1$. Then C_1 and C_2 are isomorphic over $\mathbb{F}$ if and only if there exist $s \in \mathbb{F}^\star$, $t \in \mathbb{F}$, and $r(u) \in \mathbb{F}[u]$ with $\deg(r(u)) \le g$, such that H_1 can be transformed into H_2 through the coordinate change:

$$(u, v) \longmapsto \left(s^2u + t, s^{2g+1}v + r(u)\right). \tag{2.1}$$

In our case, a hyperelliptic curve C_q' is isomorphic to the hyperelliptic curve C_q if and only if there exist $s \in \mathbb{F}_q^*$ and $t \in \mathbb{F}_q$ such that C_q' has the equation form

$$v^2 = u^p + s^{2(p-1)}au + s^{2p}(t^p + at + b). \tag{2.2}$$

If $q = p$, then C_q' has the equation form

$$v^2 = u^p + au + s^2((1+a)t + b), \quad s \neq 0. \tag{2.3}$$

By using (1.10), we can easily show that if C_1 and C_2 are isomorphic then their characteristic polynomials $P_1(t)$ and $P_2(t)$ are equal.

Table 2: Some cases in which C_q have reducible characteristic polynomials.

n	a	b
1	-1	0
	1	$\in \mathbb{F}_p$
	$2 < \operatorname{ord}_{\mathbb{F}_p^*}(a) < p-1$	$\in \mathbb{F}_p$
2	-1	0
	1	$\in \mathbb{F}_p$
	a primitive root of p	$\in \mathbb{F}_{p^2}$
	$2 < \operatorname{ord}_{\mathbb{F}_p^*}(a) < p-1$	$\in \mathbb{F}_{p^2}$
	$a \notin \mathbb{F}_p$, a nonprimitive root of p^2	$\in \mathbb{F}_{p^2}$
	$a \notin \mathbb{F}_p, a^{p+1} = 1$	0 or $a = b^{1-p}$

Theorem 2.1. *Let $a_0 = 1$ and*

$$C : v^2 = \sum_{i=0}^{2g+1} a_i u^{2g+1-i} \tag{2.4}$$

be a hyperelliptic curve of genus g over $\mathbb{F}_q$ of odd characteristic p, and $P(t)$ its characteristic polynomial. Let γ be a quadratic nonresidue in $\mathbb{F}_q$. Then, the hyperelliptic curve

$$C' : v^2 = \sum_{i=0}^{2g+1} \gamma^i a_i u^{2g+1-i} \tag{2.5}$$

has the characteristic polynomial $P'(t) = P(-t)$.

Proof. Let N'_j denote the number of rational points of the hyperelliptic curve C' over $\mathbb{F}_{q^j}$ and χ_j denote the extended quadratic character of $\mathbb{F}_{q^j}$. Then, since

$$\chi_j(\gamma) = \gamma^{((q-1)/2)(q^{j-1}+\cdots+q+1)} = \left(\chi_1(\gamma)\right)^{q^{j-1}+\cdots+q+1} = (-1)^j, \tag{2.6}$$

hence, according to (1.10), we have

$$\begin{aligned} N'_j &= q^j + 1 + \sum_{x\in\mathbb{F}_{q^j}} \chi_j\left(\sum_{i=0}^{2g+1} \gamma^i a_i x^{2g+1-i}\right) = q^j + 1 + \sum_{x\in\mathbb{F}_{q^j}} \chi_j\left(\sum_{i=0}^{2g+1} \gamma^i a_i (\gamma x)^{2g+1-i}\right) \\ &= q^j + 1 + \sum_{x\in\mathbb{F}_{q^j}} \chi_j(\gamma)^{2g+1} \chi_j\left(\sum_{i=0}^{2g+1} a_i x^{2g+1-i}\right) = q^j + 1 + \sum_{x\in\mathbb{F}_{q^j}} (-1)^j \chi_j\left(\sum_{i=0}^{2g+1} a_i x^{2g+1-i}\right) \\ &= \begin{cases} N_j, & j \text{ is even,} \\ 2(q^j+1) - N_j, & j \text{ is odd.} \end{cases} \end{aligned} \tag{2.7}$$

It follows $P'(t) = P(-t)$ from (1.6), (1.7), and (1.10). □

The hyperelliptic curve C' is called a *twisted curve* of C over $\mathbb{F}_q$ by γ. For the curve C_q, its twisted curve is a hyperelliptic curve of the equation

$$v^2 = u^p + \gamma^{p-1} au + \gamma^p b \tag{2.8}$$

with γ a quadratic nonresidue in $\mathbb{F}_q$.

In the following, we compute the characteristic polynomials of C_q over $\mathbb{F}_q$ with $q = p^n$.

Case 1. For the curve $C_p : v^2 = u^p + au + b$ with $a = -1$ and $0 \neq b \in \mathbb{F}_p$, C_p has $(p-1)/2$ isomorphic curves over $\mathbb{F}_p$, which are

$$v^2 = u^p - u + s^2 b, \quad s = 1, 2, \cdots, \frac{(p-1)}{2}. \tag{2.9}$$

Hence, there are three isomorphism classes of hyperelliptic curves C_p over $\mathbb{F}_p$ which are denoted as $\mathcal{C}_p(-1,0)$, $\mathcal{C}_p(-1,+)$ and $\mathcal{C}_p(-1,-)$, respectively,

$$\begin{gathered} \mathcal{C}_p(-1,0) = \left\{ v^2 = u^p - u \right\}, \\ \mathcal{C}_p(-1,+) = \left\{ v^2 = u^p - u + b^+ \mid b^+ \text{ is a quadratic residue modulo } p \right\}, \\ \mathcal{C}_p(-1,-) = \left\{ v^2 = u^p - u + b^- \mid b^- \text{ is a quadratic nonresidue modulo } p \right\}. \end{gathered} \tag{2.10}$$

If $v^2 = u^p - u + b^+ \in \mathcal{C}_p(-1,+)$ and γ is a quadratic nonresidue modulo p, then its twisted curve $v^2 = u^p - \gamma^{p-1} u + \gamma^p b^+$ or $v^2 = u^p - u + \gamma b^+$ belongs to $\mathcal{C}_p(-1,-)$.

According to [9], we know that the characteristic polynomial of the hyperelliptic curve $v^2 = u^p - u$ over $\mathbb{F}_p$ is

$$P_{\mathcal{C}_p(-1,0)}(t) = \left(t^2 - \tilde{p} \right)^{(p-1)/2}. \tag{2.11}$$

While for all the curves in $\mathcal{C}_p(-1,+)$ or $\mathcal{C}_p(-1,-)$, their characteristic polynomials were proved by Duursma [9] to be

$$\prod_{k=1}^{p-1} \left(t - \left(\frac{k}{p} \right) \zeta^k \sqrt{\tilde{p}} \right) \quad \text{or} \quad \prod_{k=1}^{p-1} \left(t + \left(\frac{k}{p} \right) \zeta^k \sqrt{\tilde{p}} \right), \tag{2.12}$$

respectively.

For examples, the curve $v^2 = u^5 - u$ over $\mathbb{F}_5$ and the curve $v^2 = u^7 - u$ over $\mathbb{F}_7$ have the characteristic polynomial $(t^2 - 5)^2$ and $P(t) = (t^2 + 7)^3$, respectively. The curves in $\mathcal{C}_5(-1,+)$ or $\mathcal{C}_7(-1,+)$ have the characteristic polynomial $t^4 + 5t^3 + 15t^2 + 25t + 25$ or $t^6 + 7t^5 + 21t^4 + 49t^3 + 147t^2 + 343t + 343$, respectively. The curves in $\mathcal{C}_5(-1,-)$ or $\mathcal{C}_7(-1,-)$ have the characteristic polynomial $t^4 - 5t^3 + 15t^2 - 25t + 25$ or $t^6 - 7t^5 + 21t^4 - 49t^3 + 147t^2 - 343t + 343$, respectively.

Case 2. Over $\mathbb{F}_{p^2}$, the hyperelliptic curve $v^2 = u^p + u$ is a quotient of the Hermitian curve $v^{p+1} = u^p + u$ which is maximal, and this leads to that over $\mathbb{F}_{p^2}$, $v^2 = u^p + u$ has the characteristic polynomial [10]

$$P(\mathrm{t}) = (t+p)^{p-1}. \tag{2.13}$$

Based on the following Theorem 2.6, for any $b \in \mathbb{F}_p$, the curve $v^2 = u^p + u + b$ is isomorphic to $v^2 = u^p + u$. Thus, $v^2 = u^p + u + b$ over $\mathbb{F}_{p^2}$ also has the characteristic polynomial (2.13). And it follows that the characteristic polynomial of $v^2 = u^p + u + b$ over $\mathbb{F}_p$ equals to

$$P(\mathrm{t}) = \left(t^2 + p\right)^{(p-1)/2}. \tag{2.14}$$

Case 3. Suppose $a \neq 0, \pm 1$. Then for the fixed a and all $b \in \mathbb{F}_p$, all the hyperelliptic curves $v^2 = u^p + au + b$ are isomorphic. Hence, each of these curves is isomorphic to its twisted curve. Thus, the coefficients of the terms of odd degrees in their corresponding characteristic polynomials are zero. In fact, we have the following Lemma 2.2.

Lemma 2.2. *Suppose p is an odd prime number, $a \in \mathbb{F}_p$, and r is a positive integer satisfying $1 \leq r \leq (p-1)/2$. Then*

$$\sum_{x\in\mathbb{F}_{p^r}} \chi_r(x^p + ax) = 0 \tag{2.15}$$

holds if one of the following three conditions is satisfied:

(1) $r = 2$ *or* r *is odd;*

(2) $r(> 2)$ *is even and* a *is a primitive root modulo* p.

Proof. Suppose r is odd, and let γ be a quadratic nonresidue in $\mathbb{F}_p$. Then, we have

$$\begin{aligned}\sum_{x\in\mathbb{F}_{p^r}} \chi_r(x^p + ax) &= \sum_{x\gamma\in\mathbb{F}_{p^r}} \chi_r\left((x\gamma)^p + ax\gamma\right) \\ &= \sum_{x\in\mathbb{F}_{p^r}} \chi_r(\gamma)\chi_r(x^p + ax) = (-1)^r \sum_{x\in\mathbb{F}_{p^r}} \chi_r(x^p + ax) \\ &= -\sum_{x\in\mathbb{F}_{p^r}} \chi_r(x^p + ax),\end{aligned} \tag{2.16}$$

and it follows $\sum_{x\in\mathbb{F}_{p^r}} \chi_r(x^p + ax) = 0$.

Let $r = 2$ or r even and a a primitive root modulo p. We first show that $x^p + ax$ will run through $\mathbb{F}_{p^r}$ if x runs through $\mathbb{F}_{p^r}$. It is equivalent to show that for any $x \in \mathbb{F}_{p^r}$, if $x \neq 0$, then $x^p + ax \neq 0$. That is, we have to show that the equation $x^p + ax = 0$ has no nonzero solution in $\mathbb{F}_{p^r}$.

Assume that x_0 is a nonzero root of $x^p + ax = 0$ in $\mathbb{F}_{p^r}$, that is, $\text{x}_0^p = -ax_0$. Then we have $x_0^{p^2} = -ax_0^p = (-1)^2 a^2 x_0$, and it follows $x_0^{p^r} = (-a)^{r-1} x_0^p = (-1)^r a^r x_0$, that is, $x_0 = a^r x_0$ or $x_0(1 - a^r) = 0$. Thus, $x_0 = 0$ or $a^r = 1$, it is impossible. Therefore,

$$\sum_{x \in \mathbb{F}_{p^r}} \chi_r(x^p + ax) = \sum_{x \in \mathbb{F}_{p^r}} \chi_r(x) = 0. \tag{2.17}$$

□

Lemma 2.3. *For any odd prime number p, we have*

$$\sum_{x \in \mathbb{F}_{p^r}} \chi_r(x^p + x) = \begin{cases} 0 & if\ r\ is\ odd, \\ (-1)^{r/2-1} p^{r/2}(p-1) & if\ r\ is\ even\ and\ no\ larger\ than\ p. \end{cases} \tag{2.18}$$

Proof. $\sum_{x \in \mathbb{F}_{p^r}} \chi_r(x^p + x) = 0$ comes directly from Lemma 2.2 if r is odd.

Suppose r is even and $r \leq p - 1$. Let $a_k (0 \leq k \leq p - 1)$ be the coefficients of the characteristic polynomial (2.14); then $a_k = 0$ if k is odd, and

$$a_k = p^{k/2} \cdot \frac{(p-1)(p-3)\cdots(p-k+1)}{2^{k/2} \cdot (k/2)!} \tag{2.19}$$

if k is even. Thus, from (1.7), we have

$$ka_k = \sum_{x \in \mathbb{F}_{p^k}} \chi_k(x^p + x) + a_2 \sum_{x \in \mathbb{F}_{p^{k-2}}} \chi_{k-2}(x^p + x) + \cdots + a_{k-2} \sum_{x \in \mathbb{F}_{p^2}} \chi_2(x^p + x). \tag{2.20}$$

From this above equation and (2.19), we can inductively show

$$\sum_{x \in \mathbb{F}_{p^r}} \chi_r(x^p + x) = (-1)^{r/2-1} p^{r/2}(p-1). \tag{2.21}$$

□

Theorem 2.4. *Suppose p is an odd prime number and $a(\neq 0, \pm 1) \in \mathbb{F}_p$. Let m be the order of a in the multiplicative group $\mathbb{F}_p^*$. Then, the characteristic polynomial of the curve $v^2 = u^p + au + b$ over $\mathbb{F}_p$ is*

$$P(t) = \begin{cases} \left(t^m + \left(\dfrac{-1}{p}\right)(-p)^{m/2}\right)^{(p-1)/m} & if\ m\ is\ even, \\ \left(t^{2m} + p^m\right)^{(p-1)/2m} & if\ m\ is\ odd. \end{cases} \tag{2.22}$$

Proof. Since $v^2 = u^p + au + b$ is isomorphic to $v^2 = u^p + au$, we only have to consider the curve $v^2 = u^p + au$ over $\mathbb{F}_p$.

Let $p - 1 = ml$, then $a^{mk} = 1$ for $k = 1, 2, \ldots, l$. For any even positive integer r not divided by m, since $a^r \neq 1$, the mapping $x \mapsto x^p + ax$ is a one-to-one mapping in $\mathbb{F}_{p^r}$, hence, we have

$$\sum_{x \in \mathbb{F}_{p^r}} \chi_r(x^p + ax) = \sum_{x \in \mathbb{F}_{p^r}} \chi_r(x) = 0. \tag{2.23}$$

It follows that $a_r = 0$ based on (1.7) and Lemma 2.2. Thus, for all positive integer r satisfying $r \nmid m$, the coefficients a_r of $v^2 = u^p + au$'s characteristic polynomial are equal to 0.

Let θ be a generator of the cyclic multiplicative group $\mathbb{F}_{p^m}^*$, then there exists an integer $k(1 < k < (p^m - 1)/2)$ such that $(p^m - 1)/m \mid k$ and $a = \theta^k$, and it follows that there exists an integer r satisfying $1 \leq r \leq m - 1$, $(r, m) = 1$ and

$$\left(\theta^{r(\sum_{i=0}^{m-1} p^i/m)}\right)^{p-1} = a. \tag{2.24}$$

Let $c = \theta^{r(\sum_{i=0}^{m-1} p^i/m)}$; then $c^{p-1} = a$ and

$$\chi_m(c^p) = (c^p)^{(p^m-1)/2} = \left(c^{p-1}\right)^{(p^{m-1}+p^{m-2}+\cdots+p+1)/2} = a^{(p^{m-1}+p^{m-2}+\cdots+p+1)/2}. \tag{2.25}$$

From $p - 1 = ml$ or $p = ml + 1$, we know that there exist integers s_k such that

$$p^k = m^2 l^2 s_k + kml + 1, \tag{2.26}$$

and it follow that there exists an integer s such that

$$\sum_{k=0}^{m-1} p^k = m^2 l^2 s + \frac{m(m-1)}{2} \cdot ml + m. \tag{2.27}$$

If m is even, then we have

$$\frac{(p^{m-1} + p^{m-2} + \cdots + p + 1)}{2} \equiv \frac{m^2(m-1)l}{4} + \frac{m}{2} \bmod m. \tag{2.28}$$

Hence,

$$\chi_m(c^p) = a^{\sum_{k=0}^{m-1} p^k/2} = \left(a^{m/2}\right)^{(m-1)ml/2+1} = (-1)^{(m-1)ml/2+1} = (-1)^{ml/2+1} = (-1)^{(p+1)/2}. \tag{2.29}$$

Thus, from (2.21), we have

$$\begin{aligned}\sum_{x\in\mathbb{F}_{p^m}} \chi_m(x^p + ax) &= \sum_{x\in\mathbb{F}_{p^m}} \chi_m\left(c^p\left(\left(\frac{x}{c}\right)^p + \frac{a}{c^{p-1}} \cdot \frac{x}{c}\right)\right) = \chi_m(c^p) \sum_{x\in\mathbb{F}_{p^m}} \chi_m\left(\left(\frac{x}{c}\right)^p + \frac{x}{c}\right) \\ &= \chi_m(c^p) \sum_{x\in\mathbb{F}_{p^m}} \chi_m(x^p + x) = (-1)^{(p+m-1)/2} p^{m/2}(p-1).\end{aligned} \tag{2.30}$$

In addition, for any positive integer k, we have

$$\chi_{mk}(c^p) = (c^p)^{(p^{mk}-1)/2} = (-1)^{(p+1)k/2}. \tag{2.31}$$

And so for $k \le (p-1)/m$, based on (2.21), we have

$$\sum_{x\in\mathbb{F}_{p^{mk}}} \chi_{mk}(x^p+ax) = \sum_{x\in\mathbb{F}_{p^{mk}}} \chi_{mk}\left(c^p\left(\left(\frac{x}{c}\right)^p + \frac{a}{c^{p-1}}\cdot\frac{x}{c}\right)\right) = \chi_{mk}(c^p)\sum_{x\in\mathbb{F}_{p^{mk}}} \chi_{mk}\left(\left(\frac{x}{c}\right)^p + \frac{x}{c}\right)$$
$$= \chi_{mk}(c^p)\sum_{x\in\mathbb{F}_{p^{mk}}} \chi_{mk}(x^p+x) = (-1)^{(p+1+m)k/(2-1)} p^{mk/2}(p-1). \tag{2.32}$$

Therefore, for $k = 1,\ldots,\lfloor (p-1)/2m \rfloor$, we have the coefficients a_{mk} of the corresponding characteristic polynomial $P(t)$ as follows:

$$a_{mk} = \left(\frac{-1}{p}\right)^k \binom{(p-1)/m}{k} (-p)^{mk/2}. \tag{2.33}$$

Hence, the characteristic polynomial for even m is

$$P(t) = \left(t^m + \left(\frac{-1}{p}\right)(-p)^{m/2}\right)^{(p-1)/m}. \tag{2.34}$$

Especially, if a is a primitive element modulo p, we have

$$P(t) = t^{p-1} + p^{(p-1)/2}. \tag{2.35}$$

Suppose m is odd. Then $2m \mid (p-1)$ and $2m$ is the smallest even positive integer satisfying $a^{2m} = 1$. According to the equalities (2.25) and (2.27), we have

$$\chi_{2m}(c^p) = (c^p)^{(p^{2m}-1)/2} = \left(c^{p-1}\right)^{p\sum_{i=0}^{2m-1} p^i/2} = (a^m)^{\sum_{i=0}^{2m-1} p^i/2m} = 1, \tag{2.36}$$

where $c = \theta^{r_1(\sum_{i=0}^{2m-1} p^i/2m)}$ for some integer r_1. And it follows that $\chi_{2mk}(c^p) = 1$ holds for any positive integer k.

Since for any odd integer k, we have $a_{mk} = 0$. Hence, similar to the proof of the formula (2.21), for any positive integer $k(1 \le k \le \lfloor (p-1)/4m \rfloor)$, we have

$$\sum_{x\in\mathbb{F}_{p^{2mk}}} \chi_{2mk}(x^p+ax) = (-1)^{k-1} p^{mk}(p-1). \tag{2.37}$$

Hence, the corresponding characteristic polynomial coefficient a_{2mk} for $1 \le k \le \lfloor (p-1)/4m \rfloor$ equals to

$$\binom{(p-1)/2m}{k} p^{mk}. \tag{2.38}$$

Thus, the corresponding characteristic polynomial is

$$P(t) = \sum_{k=0}^{(p-1)/2m} \binom{(p-1)/2m}{k} (p^m)^k t^{(p-1)-2mk} = \left(t^{2m} + p^m\right)^{(p-1)/2m}. \tag{2.39}$$

□

For example, let $p = 13$, then $a = 5$ is not a primitive root of modulo $p = 13$. In fact, we have $5^4 \equiv 1 \bmod 13$, and the characteristic polynomial of the curve $v^2 = u^{13} + 5u$ over $\mathbb{F}_{13}$ is $(t^4 + 169)^3$.

Case 4. Now we consider the curves $v^2 = u^p + au + b$ over $\mathbb{F}_{p^2}$.

Theorem 2.5. *Suppose p is an odd prime number.*

(1) *The curve $v^2 = u^p - u$ over $\mathbb{F}_{p^2}$ has the characteristic polynomial*

$$(t - \tilde{p})^{p-1}. \tag{2.40}$$

(2) *For any nonzero element $b \in \mathbb{F}_{p^2}$, the all roots of the equation*

$$x^p - x + b - 2^{-1}(b + b^p) = 0 \tag{2.41}$$

are in $\mathbb{F}_{p^2}$. Therefore, for every nonzero element $b \in \mathbb{F}_{p^2}$, the hyperelliptic curve $v^2 = u^p - u + b$ over $\mathbb{F}_{p^2}$ has the characteristic polynomial

$$\prod_{\zeta^p=1, \zeta \neq 1} (t - \zeta\tilde{p}). \tag{2.42}$$

Proof. (1) If $x^p - x \neq 0$ for $x \in \mathbb{F}_{p^2}$, then we have

$$(x^p - x)^{(p^2-1)/2} = \left((x^p - x)^p (x^p - x)^{-1}\right)^{(p+1)/2} = (-1)^{(p+1)/2} = -\left(\frac{-1}{p}\right). \tag{2.43}$$

Hence,

$$\sum_{x \in \mathbb{F}_{p^2}} \chi_2(x^p - x) = \left(p^2 - p\right)\left(-\left(\frac{-1}{p}\right)\right). \tag{2.44}$$

It follows that if α_i $(i = 1, \ldots, p-1)$ are the all roots of the characteristic polynomial of $v^2 = u^p - u$ over $\mathbb{F}_{p^2}$, then

$$\sum_{i=1}^{p-1} \alpha_i = \left(p^2 - p\right)\left(\frac{-1}{p}\right) = (p-1)\left(\left(\frac{-1}{p}\right)p\right), \tag{2.45}$$

and so we have

$$\sum_{i=1}^{(p-1)/2}\left(\alpha_i+\overline{\alpha_i}-2\left(\frac{-1}{p}\right)p\right)=0,\quad \alpha_i\overline{\alpha_i}=p^2. \tag{2.46}$$

It follows $\alpha_i=(-1/p)p=\widetilde{p}$ for $i=1,2,\ldots,(p-1)/2$. Hence, the characteristic polynomial of the curve $v^2=u^p-u$ over $\mathbb{F}_{p^2}$ is

$$(t-\widetilde{p})^{p-1}. \tag{2.47}$$

(2) Let β be a root of $x^p-x+b-2^{-1}(b+b^p)=0$, then $\beta^p=\beta-b+2^{-1}(b+b^p)$, and it follows $\beta^{p^2}=\beta$, which means $\beta\in\mathbb{F}_{p^2}$.

For any element $b(\neq 0)$ in $\mathbb{F}_{p^2}$, let s be a root of the equation $x^2=2(b+b^p)^{-1}$ in $\mathbb{F}_{p^2}$ and t a root of $x^p-x+b-2^{-1}(b+b^p)=0$. Then $s,t\in\mathbb{F}_{p^2}$, and so the curve $v^2=u^p-u+b$ is isomorphic to $v^2=u^p-u+1$. Hence, for any nonzero element $b\in\mathbb{F}_{p^2}$, all the curve $v^2=u^p-u+b$ has the characteristic polynomial

$$\prod_{\zeta^p=1,\zeta\neq 1}(t-\zeta\widetilde{p}). \tag{2.48}$$

□

For example, let ν be a root of $u^2+u+2=0$ mod 5, then the curve $C_{-1,\nu}$: $v^2=u^5-u+\nu$ over $\mathbb{F}_{5^2}$ has the characteristic polynomial

$$\begin{aligned}P(t)&=\prod_{\zeta^p=1,\zeta\neq 1}\left(t-\zeta\left(\frac{-1}{5}\right)5\right)\\&=t^4+5t^3+25t^2+125t+625.\end{aligned} \tag{2.49}$$

Since ν is a quadratic nonresidue in $\mathbb{F}_{5^2}$, the curve $C'_{-1,\nu}$:

$$v^2=u^5-\nu^4u+\nu^6\quad \text{or } v^2=u^5-(2+3\nu)u+2 \tag{2.50}$$

is one twisted curve of $C_{-1,\nu}$. Hence, $C'_{-1,\nu}$'s characteristic polynomial is

$$P'(t)=t^4-5t^3+25t^2-125t+625. \tag{2.51}$$

Suppose ξ is a root of $x^2+x+3=0$ mod 7. Then the curve $C_{-1,\xi}$: $v^2=u^7-u+\xi$ over $\mathbb{F}_{7^2}$ has the characteristic polynomial

$$P(t)=t^6-7t^5+49t^4-343t^3+2401t^2-16807t+117649. \tag{2.52}$$

Since ξ is a quadratic nonresidue in $\mathbb{F}_{7^2}$, the curve $C'_{-1,\xi}$:

$$v^2=u^7-(4+5\xi)u+3\quad \text{over } \mathbb{F}_{7^2} \tag{2.53}$$

is one twisted curve of $C_{-1,\xi}$. $C'_{-1,\xi}$ has the characteristic polynomial

$$P'(t) = t^6 + 7t^5 + 49t^4 + 343t^3 + 2401t^2 + 16807t + 117649. \tag{2.54}$$

Theorem 2.6. *Suppose p is an odd prime number. Then,*

(1) *the equation*

$$x^p + x + b = 0 \tag{2.55}$$

has roots in $\mathbb{F}_{p^2}$ if and only if $b \in \mathbb{F}_p$.

For any $b \in \mathbb{F}_{p^2}$, the curve $v^2 = u^p + u + b = 0$ is isomorphic to the curve $v^2 = u^p + u$ over $\mathbb{F}_{p^2}$ if and only if $b \in \mathbb{F}_p$.

(2) For any $b, c \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, the curve $v^2 = u^p + u + b$ is isomorphic to the curve $v^2 = u^p + u + c$ over $\mathbb{F}_{p^2}$.

Proof. (1) Suppose $b \in \mathbb{F}_p$ and $x_0 \in \mathbb{F}_{p^{2p}}$ is a root of $u^p + u + b = 0$. Then, $x_0^p = -x_0 - b$ and it follows $x_0^{p^2} = x_0$, which implies $x_0 \in \mathbb{F}_{p^2}$. On the other hand, if x_0 is a root of $u^p + u + b = 0$ in $\mathbb{F}_{p^2}$, then $b - b^p = 0$, which implies $b \in \mathbb{F}_p$.

Let x_0 be a root of $v^2 = u^p + u + b = 0$ in $\mathbb{F}_{p^{2p}}$, then $x_0 \in \mathbb{F}_{p^2}$, and over $\mathbb{F}_{p^2}$, the curve $v^2 = u^p + u + b$ is isomorphic to the curve $v^2 = u^p + u + (x_0^p + x_0 + b)$, that is, $v^2 = u^p + u$.

(2) Suppose b and c are two different elements in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Then, obviously, $(c - c^p)(b - b^p)^{-1} \in \mathbb{F}_p$. Let s be a square root of $(c - c^p)(b - b^p)^{-1}$ in $\mathbb{F}_{p^2}$, and let $\tilde{b} = \mathrm{b} - cs^{-2}$. Then, $\tilde{b} = (cb^p - bc^p)(c - c^p)^{-1} \in \mathbb{F}_p$.

According to (1), the equation $x^p + x + \tilde{b} = 0$ has roots in $\mathbb{F}_{p^2}$. Let $t \in \mathbb{F}_{p^2}$ be a root of $x^p + x + \tilde{b} = 0$; then, over $\mathbb{F}_{p^2}$, the curve $v^2 = u^p + u + b$ is isomorphic to the curve

$$v^2 = u^p + s^{2(p-1)}u + s^{2p}(t^p + t + b). \tag{2.56}$$

That is, $v^2 = u^p + u + b$ is isomorphic to $v^2 = u^p + u + c$ over $\mathbb{F}_{p^2}$ since we have

$$s^{2(p-1)} = 1, \qquad s^{2p}(t^p + t + b) = s^2\left(-\tilde{b} + b\right) = s^2\left(cs^{-2}\right) = c. \tag{2.57}$$

□

For any $b \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, the curve $v^2 = u^p + u + b$ has the same characteristic polynomial.

Theorem 2.7. *Suppose p is an odd prime number and $b \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. If $p \equiv 1 \mod 4$, then for every $b \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, the curve $v^2 = u^p + u + b$ is a twisted curve of some curve of the form $v^2 = u^p - u + b'$ with $b' \in \mathbb{F}_{p^2}$. If $p \equiv -1 \mod 4$, then for every $b \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, the curve $v^2 = u^p + u + b$ is isomorphic to the curve $v^2 = u^p - u + 1$ over $\mathbb{F}_{p^2}$.*

Hence, over $\mathbb{F}_{p^2}$, the characteristic polynomial of the curve $v^2 = u^p + u + b$ with $b \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ is

$$\prod_{\zeta^p = 1, \zeta \neq 1} (t + \zeta p). \tag{2.58}$$

Proof. Let θ be a generator of the cyclic multiplicative group $\mathbb{F}_{p^2}^*$.

(1) Assume $p \equiv 1 \mod 4$. Set $\gamma = \theta^{(p+1)/2}$; then

$$\gamma^{p-1} = \left(\theta^{(p+1)/2}\right)^{p-1} = -1, \qquad \gamma^p = -\gamma, \qquad \chi(\gamma) = \left(\theta^{(p^2-1)/2}\right)^{(p+1)/2} = (-1)^{(p+1)/2} = -1. \tag{2.59}$$

It follows that γ is a quadratic nonresidue in $\mathbb{F}_{p^2}$, and the curve $v^2 = u^p + u + b$ is a twist of the curve $v^2 = u^p - u - \theta^{(2p-3)(p+1)/2} b$. Hence, due to Theorems 2.1 and 2.5, the curve $v^2 = u^p + u + b$ has the characteristic polynomial

$$\prod_{\zeta^p=1,\zeta\neq 1} \left(-t - \zeta\tilde{p}\right) \quad \text{or} \quad \prod_{\zeta^p=1,\zeta\neq 1} \left(t + \zeta\tilde{p}\right). \tag{2.60}$$

(2) Assume $p \equiv -1 \mod 4$. Let $s = \theta^{(p-2)(p+1)/4}$, $t = 0$, and $b = \theta^{(p+1)/2}$. Then, $s, b \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, and the curve $v^2 = u^p + u + b$ is isomorphic to the curve

$$v^2 = u^p + s^{2(p-1)} u + s^{2p} b. \tag{2.61}$$

It follows that $v^2 = u^p + u + b$ is isomorphic to the curve $v^2 = u^p - u + 1$ since $s^{2(p-1)} = -1$ and $s^{2p} b = \theta^{-(p+1)/2} b = 1$. Therefore, for every $b \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, the curve $v^2 = u^p + u + b$ has the same characteristic polynomial as the curve $v^2 = u^p - u + 1$ over $\mathbb{F}_{p^2}$, that is,

$$\prod_{\zeta^p=1,\zeta\neq 1} \left(t - \zeta\tilde{p}\right). \tag{2.62}$$

In a word, for any odd prime number, the characteristic polynomial of the curve $v^2 = u^p + u + b$ is

$$\prod_{\zeta^p=1,\zeta\neq 1} \left(t + \left(\frac{-1}{p}\right)\zeta\tilde{p}\right) \quad \text{or} \quad \prod_{\zeta^p=1,\zeta\neq 1} \left(t + \zeta p\right). \tag{2.63}$$

□

Theorem 2.8. *Suppose p is an odd prime number, $a, b \in \mathbb{F}_{p^2}$, and $a \neq 0, \pm 1$. Let m be the order of a in $\mathbb{F}_p^*$ if $a \in \mathbb{F}_p$, that is, $m = \operatorname{ord}_{\mathbb{F}_p^*}(a)$. And let $m = \operatorname{ord}_{\mathbb{F}_{p^2}^*}(a)$ and $e(>1)$ be the smallest positive integer such that $m \mid e(p+1)$ if $a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$.*

(1) *Suppose $a^{p+1} = 1$. Then $a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, and the characteristic polynomial is*

$$P(t) = \begin{cases} \left(t + a^{(p+1)/2} p\right)^{p-1} & \textit{if } b \neq 0,\ a = b^{1-p},\ \textit{or } b = 0, \\ \displaystyle\prod_{\zeta^p=1,\zeta\neq 1} \left(t + \zeta p\right) & \textit{if } a \neq b^{1-p}. \end{cases} \tag{2.64}$$

(2) *Suppose* $a^{p+1} \neq 1$; *then the characteristic polynomial of the curve* $v^2 = u^p + au + b$ *over* $\mathbb{F}_{p^2}$ *is*

$$P(t) = \begin{cases} \left(t^{(p-1)/2} + p^{(p-1)/2}\right)^2 & if\ a \in \mathbb{F}_p,\ m = p-1, \\ \left(t^{m/2} + \left(\dfrac{-1}{p}\right)(-p)^{m/2}\right)^{2(p-1)/m} & if\ a \in \mathbb{F}_p,\ m < p-1,\ m\ is\ even, \\ \left(t^m + p^m\right)^{(p-1)/m} & if\ a \in \mathbb{F}_p,\ m < p-1,\ m\ is\ odd, \\ \left(t^e + (-1)^{e(p+1)/m+e-1} p^e\right)^{(p-1)/e} & if\ a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p. \end{cases} \tag{2.65}$$

Proof. (1) If $a^{p+1} = 1$, then $a \notin \mathbb{F}_p$ since $a^2 \neq 1$. Let θ be a generator of the cyclic multiplicative group $\mathbb{F}_{p^2}$. Then, there exists an integer e satisfying $1 \leq e \leq p$, $e \neq (p+1)/2$, and $a = \theta^{e(p-1)}$.

If $a^{(p+1)/2} = -1$, then e is odd. Let $\gamma = \theta^{p+1-e}$, then

$$\gamma^{(p^2-1)/2} = \theta^{(p+1-e)(p^2-1)/2} = \theta^{-e(p^2-1)/2} = \left(\theta^{(p^2-1)/2}\right)^{-e} = (-1)^e = -1; \tag{2.66}$$

it means that γ is a quadratic nonresidue in $\mathbb{F}_{p^2}$. Hence, the curve $v^2 = u^p + au + b$ has a twisted curve defined by the equation

$$v^2 = u^p + \gamma^{p-1} au + \gamma^p b, \quad \text{that is, } v^2 = u^p + u + \theta^{p+1-ep} b. \tag{2.67}$$

If $\theta^{p+1-ep} b \in \mathbb{F}_p$, then $b = 0$, or $b \neq 0$ and $(\theta^{p+1-ep} b)^{p-1} = 1$ which means $a = b^{1-p}$. Hence, the curve $v^2 = u^p + u + \theta^{p+1-ep} b$ is isomorphic to the curve $v^2 = u^p + u$. Thus, over $\mathbb{F}_{p^2}$, the curve $v^2 = u^p + au + b$ has the characteristic polynomial $(-t+p)^{p-1}$, that is, $(t-p)^{p-1}$.

If $\theta^{p+1-ep} b \notin \mathbb{F}_p$, that is, $b \neq 0$ and $a \neq b^{1-p}$, then according to Theorem 2.7, $v^2 = u^p + u + \theta^{p+1-ep} b$ has the characteristic polynomial $\prod_{\zeta^p=1, \zeta \neq 1}(t + \zeta p)$.

If $a^{(p+1)/2} = 1$, then e is even. Let $s = \theta^{e/2}$ and $t = 0$, then the curve $v^2 = u^p + au + b$, that is,

$$v^2 = u^p + s^{2(p-1)} u + s^{2p}(t^p + t + b_1) \tag{2.68}$$

is an isomorphic curve of the curve

$$v^2 = u^p + u + b_1 \quad \text{with } b_1 = s^{-2p} b = \theta^{-ep} b. \tag{2.69}$$

It is clear that $b_1 = \theta^{-ep} b \in \mathbb{F}_p$ if and only if $a = b^{1-p}$. Hence, based on Theorems 2.6 and 2.7, the curve $v^2 = u^p + au + b$ has the characteristic polynomial

$$(t+p)^{p-1} \quad \text{for } a = b^{1-p} \quad \text{or} \quad \prod_{\zeta^p=1, \zeta \neq 1} (t + \zeta p) \quad \text{for } a \neq b^{1-p}. \tag{2.70}$$

For $b = 0$, we can also show our result as follows.

Set $\alpha_k = \theta^{e+(p+1)(2k+1)/2}$ with $0 \leq k \leq p-2$. Then, α_k are the $p-1$ different nonzero roots of $x^p + ax = 0$ in $\mathbb{F}_{p^2}$. Hence, if x is a nonzero root of $x^p + ax = 0$ in $\mathbb{F}_{p^2}$, we have

$$\begin{aligned}\chi_1^*(x^p + ax) &= (x^p + ax)^{(p^2-1)/2} = \left((x^p + ax)^p (x^p + ax)^{-1}\right)^{(p+1)/2} \\ &= \left(a^p (ax + x^p)(x^p + ax)^{-1}\right)^{(p+1)/2} = \left(a^{(p+1)/2}\right)^p = a^{(p+1)/2}.\end{aligned} \tag{2.71}$$

Thus, according to (1.4) and (1.10), each root of the corresponding characteristic polynomial equals to $-a^{(p+1)/2}p$. It follows that the corresponding characteristic polynomial is

$$P(t) = \left(t + a^{(p+1)/2}p\right)^{p-1}. \tag{2.72}$$

(2) If $a^{p+1} \neq 1$, then $(1 - a^{p+1})^{-1}(a^p b - b^p)$ is a root of $u^p + au + b = 0$. Set $s = 1$ and $t = (1 - a^{p+1})^{-1}(a^p b - b^p)$, then, over the field $\mathbb{F}_{p^2}$, $v^2 = u^p + au + b$ is isomorphic to $v^2 = u^p + s^{2(p-1)} au + s^{2p}(t^p + at + b)$, that is, $v^2 = u^p + au$. Hence, we only have to compute the characteristic polynomial of the curve $v^2 = u^p + au$ over $\mathbb{F}_{p^2}$.

(i) If $a \in \mathbb{F}_p$, then $a^{p+1} \neq 1$ means $a \neq \pm 1$. Suppose a is a primitive root of p; then the equation $x^p + ax = 0$ has only zero root in $\mathbb{F}_{p^{2r}}$ for any positive integer $r : 1 \leq 1 \leq (p-3)/2$, and it follows that the r-th coefficient a_r of the characteristic polynomial of $v^2 = u^p + au$ is 0.

Now we compute the $(p-1)/2$-th coefficient $a_{(p-1)/2}$. Let θ be a generator of the cyclic multiplicative group $\mathbb{F}^*_{(p^2)^{(p-1)/2}}$; then there exists an integer r satisfying $1 \leq r \leq p-2$, $(r, p-1) = 1$, and $(\theta^{r(\sum_{i=0}^{p-2} p^i / p-1)})^{p-1} = a$.

Set $c = \theta^{r(\sum_{i=0}^{p-2} p^i/(p-1))}$; then $c \in \mathbb{F}^*_{p^{p-1}}$, $c^{p-1} = a$, and $\chi^*_{(p-1)/2}(c^p) = \chi_{p-1}(c^p) = (-1)^{(p+1)/2}$. Hence, based on Lemma 2.3, we have

$$\begin{aligned}\sum_{x \in \mathbb{F}_{(p^2)^{(p-1)/2}}} \chi^*_{(p-1)/2}(x^p + ax) &= \sum_{x \in \mathbb{F}_{(p^2)^{(p-1)/2}}} \chi^*_{(p-1)/2}\left(c^p\left(\left(\frac{x}{c}\right)^p + \frac{a}{c^{p-1}} \cdot \frac{x}{c}\right)\right) \\ &= \chi_{p-1}(c^p) \sum_{x \in \mathbb{F}_{p^{p-1}}} \chi_{p-1}(x^p + x) = (-1)^{(p+1)/2}(-1)p^{(p-1)/2}(p-1) \\ &= p^{(p-1)/2}(p-1),\end{aligned} \tag{2.73}$$

where χ_k^* denotes the extended quadratic character of the degree k extension of $\mathbb{F}_{p^2}$ (i.e., $\mathbb{F}_{p^{2k}}$), which is equivalent to χ_{2k}, the extended quadratic character of the degree $2k$ extension of $\mathbb{F}_p$. Thus,

$$a_{(p-1)/2} = \frac{1}{(p-1)/2} \cdot p^{(p-1)/2}(p-1) = 2p^{(p-1)/2}. \tag{2.74}$$

Therefore, the corresponding characteristic polynomial is

$$P(t) = t^{p-1} + 2p^{(p-1)/2}t^{(p-1)/2} + \left(p^2\right)^{(p-1)/2} = \left(t^{(p-1)/2} + p^{(p-1)/2}\right)^2. \tag{2.75}$$

(ii) Suppose $a \in \mathbb{F}_p$ and $m < p-1$; then similar to the proof of Theorem 2.4, we have the corresponding characteristic polynomial coefficients as the the following if m is even:

$$a_{mk/2} = (-1)^{(p-1)k/2}(-p)^{mk/2}\binom{2(p-1)/m}{k} \tag{2.76}$$

for $1 \leq k \leq (p-1)/m$, while the other coefficients are equal to zero. Hence, the corresponding characteristic polynomial is

$$\left(t^{m/2} + \left(\frac{-1}{p}\right)(-p)^{m/2}\right)^{2(p-1)/m}. \tag{2.77}$$

By the same way, we can show that if m is odd, the corresponding characteristic polynomial is $(t^m + p^m)^{(p-1)/m}$.

(iii) Suppose $a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, then $m \nmid (p+1)$. If an integer k satisfies $1 \leq k \leq (p-1)/2$ and $m \nmid k(p+1)$, then the corresponding characteristic polynomial is $t^{p-1} + p^{p-1}$.

Now suppose e is the smallest integer such that $2 \leq e \leq (p-1)/2$ and $m \mid e(p+1)$. Then $e \mid (p-1)$. Otherwise, let $p-1 = de + e_1$ with d being an integer and $1 \leq e_1 < e$. Then, $(p+1)(p-1) = de(p+1) + e_1(p+1)$, and it follows $m \mid e_1(p+1)$, which contradicts e being the smallest integer satisfying $m \mid e(p+1)$. Set $p-1 = el$, $e(p+1) = mt$. Clearly, $(e,t) = 1$.

For any positive integer k satisfying $e \nmid k$, since $x^p + ax = 0$ has no nonzero root in $\mathbb{F}_{p_{2k}}$, we have

$$\sum_{x\in\mathbb{F}_{(p^2)^k}} \chi_k^*(x^p + ax) = \sum_{x\in\mathbb{F}_{p^{2k}}} \chi_k^*(x) = \sum_{x\in\mathbb{F}_{p^{2k}}} \chi_{2k}(x) = 0, \tag{2.78}$$

which implies the corresponding characteristic polynomial coefficient $a_k = 0$.

Hence, we only have to compute the characteristic polynomial coefficients a_{er} for $r = 1,\ldots,\lfloor l/2 \rfloor$.

Let θ be a generator of the cyclic multiplicative group $\mathbb{F}^*_{(p^2)^e}$ or $\mathbb{F}^*_{p^{2e}}$. Then there exists an integer $k(1 \leq k \leq p^2-2)$ such that $a = \theta^{k\sum_{i=0}^{e-1}p^{2i}}$. Since $a^{e(p+1)} = 1$, we have

$$1 = \left(\theta^{k\sum_{i=0}^{e-1}p^{2i}}\right)^{e(p+1)} = \theta^{ke(p+1)\sum_{i=0}^{e-1}p^{2i}} = \theta^{(k/l)(p-1)(p+1)\sum_{i=0}^{e-1}p^{2i}} = \theta^{(k/l)(p^{2e}-1)}, \tag{2.79}$$

and it follows that k/l must be a positive integer. Set $k = lk'$, where k' is some positive integer satisfying $(e,k') = 1$ due to the smallest of e.

From $p-1=el$ or $p=el+1$, we can deduce that there exists a positive integer n such that

$$\sum_{i=0}^{e-1} p^{2i} = e^2l^2n + e^2(e-1)l + e. \tag{2.80}$$

Hence, we have

$$a = \theta^{lk'(e^2l^2n+e^2(e-1)l+e)} = \theta^{(el)k'(el^2n+e(e-1)l+1)} = \theta^{(p-1)k'(el^2n+e(e-1)l+1)}. \tag{2.81}$$

Let $\delta = \theta^{k'(el^2n+e(e-1)l+1)}$; then $a = \delta^{p-1}$, and for every integer $r : 2 \le r \le \lfloor l/2 \rfloor$, we have

$$\begin{aligned}\chi_{re}^{*}(\delta^p) &= \chi_{2re}(\delta^p) = (\delta^p)^{(p^{2re}-1)/2} = (\delta^p)^{((p^{2e}-1)/2)\sum_{i=0}^{r-1} p^{2ei}} \\ &= \left((\delta^p)^{(p^{2e}-1)/2}\right)^{\sum_{i=0}^{r-1} p^{2ei}} = \left((-1)^{e(p+1)/m}\right)^{\sum_{i=0}^{r-1} p^{2ei}} = (-1)^{re(p+1)/m}.\end{aligned} \tag{2.82}$$

And according to (2.21), we obtain

$$\begin{aligned}\sum_{x\in\mathbb{F}_{(p^2)^{re}}} \chi_{re}^{*}(x^p+ax) &= \sum_{x\in\mathbb{F}_{p^{2re}}} \chi_{2re}(x^p+ax) = \sum_{x\in\mathbb{F}_{p^{2re}}} \chi_{2re}(\delta^p)\left(\left(\frac{x}{\delta}\right)^p + \frac{a}{\delta^{p-1}}\cdot\frac{x}{\delta}\right) \\ &= \chi_{2re}(\delta^p)\sum_{x\in\mathbb{F}_{p^{2re}}} \chi_{2re}(x^p+x) = (-1)^{r(e(p+1)/m+e)-1}p^{re}(p-1).\end{aligned} \tag{2.83}$$

Therefore, the corresponding characteristic polynomial coefficient a_{re} can be computed as follows:

$$\begin{aligned}a_{re} &= \frac{1}{re}\sum_{i=0}^{r-1}\sum_{x\in\mathbb{F}_{(p^2)^{(r-i)e}}} \chi_{(r-i)e}^{*}(x^p+ax)a_{ie} \\ &= \frac{1}{re}\sum_{i=0}^{r-1}(-1)^{(r-i)(e(p+1)/m+e)-1}p^{(r-i)e}(p-1)a_{ie} \\ &= \left((-1)^{e(p+1)/m+e-1}p^e\right)^r\binom{(p-1)/e}{r},\end{aligned} \tag{2.84}$$

and it follows that the corresponding characteristic polynomial is

$$P(t) = \left(t^e + (-1)^{e(p+1)/m+e-1}p^e\right)^{(p-1)/e}. \tag{2.85}$$

□

3. Some Hyperelliptic Curves C_q Suitable for Cryptographic Applications

Due to the Pollard's rho algorithm, Index-calculus algorithm or their modified versions [11–14], the order of the Jacobian group should have a large prime factor or an almost large prime factor (i.e., the order should be a large prime times a small integer, and the hyperelliptic curves of genus greater than 3 may not be secure for cryptographic applications). Otherwise, the discrete logarithm problems on the Jacobian group may probably be solved in a subexponential time complexity or even in a polynomial time complexity. Hence, the characteristic polynomial of C_q should be irreducible over the rational number field, and the field characteristic p should be no larger than 7 when the curve C_q is considered for cryptographic uses. The following Table 2 lists some values of (n, a, b) with which C_q have reducible characteristic polynomials in rational number field and so they are not secure for cryptographic applications.

According to the Theorem 1 in [15], the curve $v^2 = u^p + u + b$ over $\mathbb{F}_p$ is supersingular and thus the parameters (the characteristic p and the extension degree of $\mathbb{F}_p$) have to be chosen carefully to defend against an MOV-type attack where the group is embedded in the multiplicative group of a finite field. Furthermore, the curves have a large automorphism group [16], and the size of the Jacobian should be large enough to defend against a parallelized Pollard rho-type attack.

If the characteristic polynomial $P(t)$ of a hyperelliptic curve C_q over $\mathbb{F}_q$ is determined, then for any positive integer m, the Jacobian group order $\#\mathbb{J}_C(\mathbb{F}_{q^m})$ can be computed as (1.8).

But if finding the roots of $P(t)$ is of some high computational complexity, then one can obtain the Jacobian group order by computing the determinant of the $(2g\times 2g)$-matrix $A^m - I$, where A is the companion matrix of $P(t)$, that is,

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & \cdots & & \cdots & \\ 0 & 0 & 0 & \cdots & 1 \\ -q^g & q^{g-1}a_1 & q^{g-2}a_2 & \cdots & a_1 \end{pmatrix}. \tag{3.1}$$

For a positive integer m, by taking $t^m - 1$ modulo $P(t)$ in the polynomial ring $\mathbb{Z}[t]$ and setting $\xi(t) = t^m - 1 \bmod P(t)$, then we get that $\xi(t)$ is a monic polynomial of degree no larger than $2g - 1$ and

$$\#\mathbb{J}_C(\mathbb{F}_{q^m}) = \prod_{i=1}^{2g}(1 - \tau_i^m) = \prod_{i=1}^{2g}\xi(\tau_i), \tag{3.2}$$

which may be another more efficient method for the computation of the Jacobian group order if the field extension degree m is very large. For C_q with $q = p$, $a = -1$, and $b(\neq 0) \in \mathbb{F}_p$, Duursma and Sakurai gave a table about the bit-sizes of the large prime factors of the orders of the Jacobian groups $\#\mathbb{J}_{C_q}(\mathbb{F}_{q^m})$ for some parameters (p, m) in [6]. In Table 3, we list some parameters (q, a, b, m) with which the Jacobian group orders $\#\mathbb{J}_{C_q}(\mathbb{F}_{q^m})$ have large prime factors, together with the corresponding characteristic polynomials, the largest prime factors,

Table 3: Some parameters for C_q whose Jacobian group orders have large prime factors.

q	m	a	b	$P(t)$	The largest prime factors of $\#\mathbb{J}_{C_q}(\mathbb{F}_{q^m})$	Bits
5	23	2,3	$b \in \mathbb{F}_5$	$t^4 + 25$	5465713352000770660547109750601	103
	29				1334402673828313149547634216455312875601	130
	37				510241095096183757930733363918820917976121	139
	43				132331554743163541916284364878460504933118649	147
	59				115740982234809846938460212895728805200607070205251\ 6944254770910797210840078500601	270
	67				867036788162169620124638326439573933801961942760108098070\ 1370016748806481465099715917129	293
	83				803692714308830143367297266327762922660863388853347980739\ 3933052864889428085088211821764213868646438952419731	362
5^2	23	1	$b \notin \mathbb{F}_p$, $b \notin \mathbb{F}_{5^2}$	$t^4 - 5t^3 + 25t^2 - 125t + 625$	529958401900871889532705668013589387152384352866888324141	189
	37				654418058067838415738219243693599843014730577527147788290\ 1122358940971377123359179724468647761	312
	41				302432661799107117404163951962923697369817504003965405048\ 43052416220664183834350299219966348767059287031	344
	43				186303988308322090874478781582395496784216892901472776234\ 2659345237037936896409322508402835718902635373797579083961	380
	53				291610525781490940421443140715914231197410552825810130042\ 681253630419471155500509947792484684708874327987628732648\ 48903982789253891086395322246881	484
	35	ν	1	$t^4 + 625$	751114601164400963558298106851275193494354988352771579238\ 818981647550964507812890001	279
	53				992546266896549276402616168146585251329055676315885009163\ 311765166575856031713035384955676431972387484913025322167\ 258482406322245836062321	459
	67				336811435885959208445641343491054920374120171960655193293\ 219265977895989598373705302211662541119647190380393508253\ 771113342078436606690357719421008432512113722632406302690\ 565490875000390001	613
7	17	3,5	$b \in \mathbb{F}_5$	$t^6 + 2401$	638991748543082113037456009420293477766438233	149
	25				101087819444250339960209489699235199115942108498312937463\ 657783601	216
	31				103602441708018848525107155829768304755490441636535691297\ 4660190950495137	240
	37				494238893933995748902489762221251946925169471844835131661\ 333855087397989688385273799604896250931261182588286429822\ 18283201	405

Table 3: Continued.

q	m	a	b	$P(t)$	The largest prime factors of $\#\mathbb{J}_{C_q}(\mathbb{F}_{q^m})$	Bits
7^2	37	-1	ξ	$t^6 - 7t^5 + 49t^4 - 343t^3 +$ $2401\mathrm{t}^2 - 16807\mathrm{t} + 117649$	91797897017374882872271724666577811943600981902942357338 6\ 99945869853906081917114280782545951467666672449434757030 0\ 5674750598455003336119	452
	23				150557819388250184737538915006485086145065087672198550975\ 2391936375710026001 37	257
	47				296622615055064026410595294739016073226621769583063595146\ 246922263428126791770055382936328803135692863434055321280\ 473083651131176444146403955371064616929027577273326083639\ 51305466751220660471713288303268418175752499584 61	730
	61	$-4 - 5\xi$	3	$t^6 - 7t^5 + 49t^4 - 343t^3 +$ $2401\mathrm{t}^2 - 16807\mathrm{t} + 117649$	8895270249059563599185595938219020670590896314104535959964\ 8016164505006377256389546604468613493539182920809346771675\ 9773506416632242948638670510523462330304278108981369417392\ 1982072102810157541240855736144227613689662410423301535608\ 9640174996978462560103065338025939666322591200406677474989	964
	71				6059483980039244877047243971289932877368693248030007997563\ 4051109664747243238974088293635840393750782605275018285648\ 0050394746490410269339276185366728255286611777338282539843\ 0750963323653238944701113108662166958149626807014450213296\ 6079886234998846359954447034509585472485237180044828118247\ 981072177295129	1013

and their bit sizes. Where "Bits" in Table 3 denotes the bit-sizes of the largest prime factors of the corresponding Jacobian group orders, ν is a root of $u^2 + u + 2 = 0 \bmod 5$ and ξ is a root of $x^2 + x + 3 = 0 \bmod 7$.

For the listed parameters (q, a, b, m) in Table 3, the corresponding Jacobian group orders are almost large primes, and so these hyperelliptic curves C_q are suitable for secure hyperelliptic curve cryptographic applications.

4. Conclusion

The computation of hyperelliptic curve Jacobian group orders is an essential step during constructing HECC. At the present, the most common method used for the computation of Jacobian group orders is by computing the zeta functions or the characteristic polynomials of the related hyperelliptic curves. Hence, computing the characteristic polynomials of hyperelliptic curves is a very useful work, and it is often a challenging work.

In this paper, we determine the characteristic polynomials of C_q over the finite field $\mathbb{F}_{p^n}$ for $n = 1, 2$ and $a, b \in \mathbb{F}_{p^n}$. By using the characteristic polynomials one can easily compute out the Jacobian group orders. And we also describe some parameters with which the Jacobian group orders of C_q have large prime factors.

The hyperelliptic curves of genus larger than 3 are not secure for cryptographic applications since the corresponding hyperelliptic curve discrete logarithm problems can be solved by the Index-calculus algorithm or its modified versions in some subexponential time. Hence, we should be careful when the curve C_q with $p > 11$ is used for practical cryptosystems. If the implementation speed is the first consideration in the construction of HECC, while the security is not in high demand, then one may choose the curve C_q with some high genus or with the Jacobian group order not having so much large prime factor. Besides, some special hyperelliptic curves having fast arithmetic over finite fields can be found efficient applications in pairing-based cryptosystems or identity-based cryptosystems ([15, 17]).

Since the (divisor) scalar multiplication computation is the most extremely time-consuming operation, we will employ the characteristic polynomials of C_q obtained here to develop some efficient scalar multiplication algorithms on C_q in our future work.

Acknowledgments

The authors would like to thank Professor Shuhong Gao for his comments which greatly improved this paper. The authors would also like to thank the anonymous referee for the careful review and the valuable comments. This research is supported by the Zhejiang Natural Science Foundation of Outstanding Youth Team Project (no. R1090138), the National Science Foundation of China (no. 60763009), and the Science and Technology Key Project of the Ministry of Education of China (no. 207089).

References

[1] N. Koblitz, "Hyperelliptic cryptosystems," *Journal of Cryptology*, vol. 1, no. 3, pp. 139–150, 1989.

[2] J. Pelzl, T. Wollinger, J. Guajardo, and C. Paar, *Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves*, vol. 2779 of *Lecture Notes in Computer Science*, Springer, Berlin, Germany, 2003.

[3] A. Weil, "Numbers of solutions of equations in finite fields," *Bulletin of the American Mathematical Society*, vol. 55, pp. 497–508, 1949.

[4] R. Hartshorne, *Algebraic Geometry*, vol. 52 of *Graduate Texts in Mathematics*, Springer, New York, NY, USA, 1977.

[5] K. S. Kedlaya, "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology," *Journal of the Ramanujan Mathematical Society*, vol. 16, no. 4, pp. 323–338, 2001.

[6] I. Duursma and K. Sakurai, "Efficient algorithms for the Jacobian variety of hyperelliptic curves $y^2 = x^p - x + 1$ over a finite field of odd characteristic p," in *Proceedings of the International Conference on Coding Theory, Cryptography and Related Areas*, pp. 73–89, Springer, Guanajuato, Mexico, 2000.

[7] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, vol. 151 of *Graduate Texts in Mathematics*, Springer, New York, NY, USA, 1994.

[8] P. Lockhart, "On the discriminant of a hyperelliptic curve," *Transactions of the American Mathematical Society*, vol. 342, no. 2, pp. 729–752, 1994.

[9] I. Duursma, "Class numbers for some hyperelliptic curves," in *Arithmetic, Geometry and Coding Theory*, pp. 45–52, de Gruyter, Berlin, Germany, 1996.

[10] S. Tafazolian, *On supersingular curves over finite fields*, Ph.D. thesis, Instituto Nacional de Matemática Pura e Aplicada, 2008.

[11] J. M. Pollard, "Carlo methods for index computation mod$p$," *Mathematics of Computation*, vol. 32, no. 143, pp. 918–924, 1978.

[12] O. Schirokauer, D. Weber, and T. Denny, "Discrete logarithms: the effectiveness of the index calculus method," in *Algorithmic Number Theory*, vol. 1122 of *Lecture Notes in Computer Science*, pp. 337–361, Springer, Berlin, Germany, 1996.

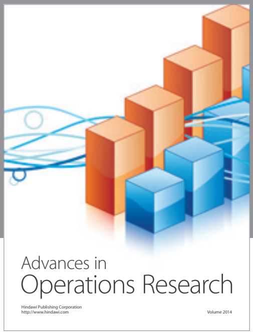
[13] P. Gaudry, "An algorithm for solving the discrete log problem on hyperelliptic curves," in *Advances in Cryptology—Eurocrypt 2000*, vol. 807 of *Lecture Notes in Computer Science*, pp. 19–34, Springer, Berlin, Germany, 2000.

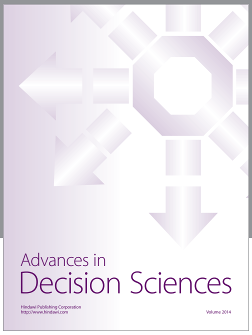
[14] P. Gaudry, E. Thomé, N. Thériault, and C. Diem, "A double large prime variation for small genus hyperelliptic index calculus," *Mathematics of Computation*, vol. 76, no. 257, pp. 475–492, 2007.

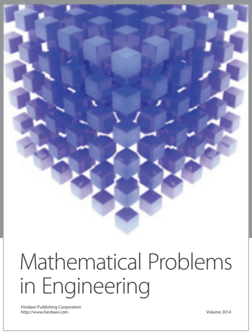
[15] S. D. Galbraith, "Supersingular curves in cryptography," in *Advances in Cryptology—ASIACRYPT 2001*, vol. 2248 of *Lecture Notes in Computer Science*, pp. 495–513, Springer, Berlin, Germany, 2001.

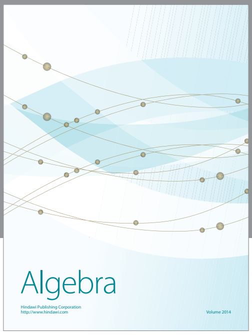
[16] H. Stichtenoth, "Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern," *Archiv der Mathematik*, vol. 24, pp. 615–631, 1973.

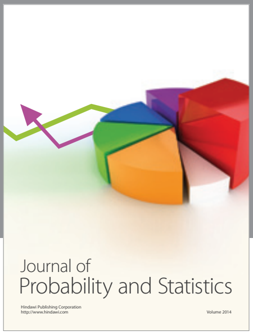
[17] D. Boneh, "A brief look at pairings based cryptography," in *Proceedings of the Annual IEEE Symposium on Foundations of Computer Science (FOCS '07)*, pp. 19–26, IEEE Press, Los Alamitos, CA, USA, 2007.


Advances in
Operations Research

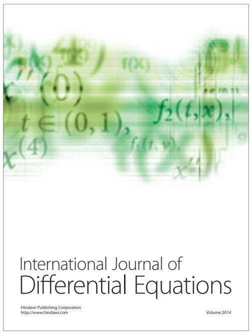

Advances in
Decision Sciences

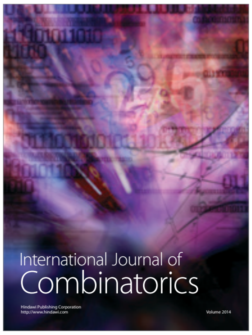

Mathematical Problems
in Engineering

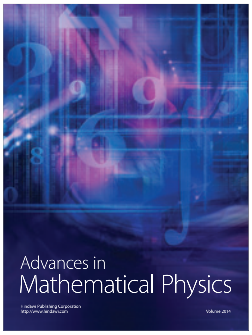

Algebra

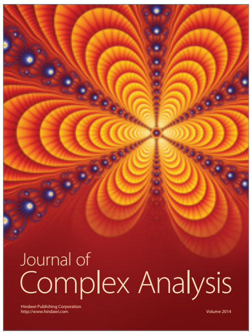

Journal of
Probability and Statistics

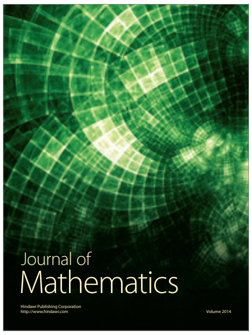
The Scientific
World Journal

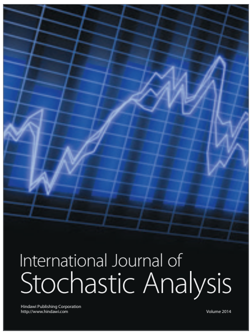

International Journal of
Differential Equations

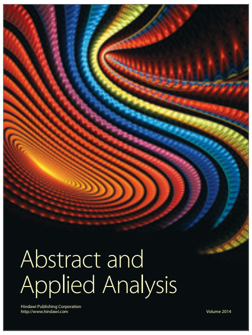

International Journal of
Combinatorics

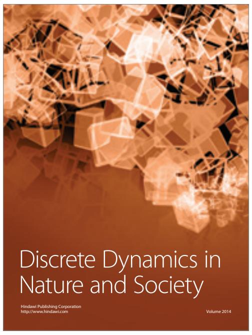

Advances in
Mathematical Physics

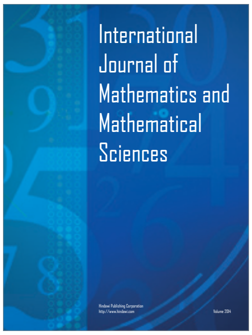

Journal of
Complex Analysis


Journal of
Mathematics


International Journal of
Stochastic Analysis

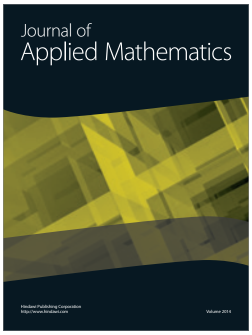

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


Journal of
Applied Mathematics

Journal of
Optimization