Isomorphism Classes of Genus-2 Hyperelliptic Curves Over Finite Fields

L. Hernández Encinas†, Alfred J. Menezes‡, and J. Muñoz Masqué†

†Instituto de Física Aplicada, CSIC, C/ Serrano 144, 28006 Madrid, Spain
E-mail: {luis, jaime}@iec.csic.es
‡Dept. of C&O, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
E-mail: ajmeneze@uwaterloo.ca

Abstract

We propose a reduced equation for hyperelliptic curves of genus 2 over finite fields $\mathbb{F}_q$ of q elements with characteristic different from 2 and 5. We determine the number of isomorphism classes of genus-2 hyperelliptic curves having an $\mathbb{F}_q$-rational Weierstrass point. These results have applications to hyperelliptic curve cryptography.

Mathematics Subject Classification 2000. Primary 11G20; Secondary 11T71, 12E20, 14H45, 14H50, 94A60.

Key words and phrases. Discriminant, hyperelliptic curves over finite fields, public-key cryptography.

Acknowledgement. †Supported by "Plan Nacional de I+D", CICYT (Spain) under grant TIC2001-0586.

1 Introduction

The *discrete logarithm problem* is the following. Given a cyclic group G of order n, a generator α of G, and an element $\beta \in G$, find the integer x, $0 \leq x \leq n-1$, such that $\beta = \alpha^x$. The importance of the discrete logarithm problem to cryptography commenced with the invention of public-key cryptography by Diffie and Hellman in 1976 [7]. Diffie and Hellman constructed a key agreement mechanism using the multiplicative group of a prime order finite field $\mathbb{Z}_p$. A large prime p and generator α of $\mathbb{Z}_p^*$ are selected as the system parameters; these quantities are public knowledge. The *security* of the scheme relies upon the difficulty of the discrete logarithm problem in the group $\mathbb{Z}_p^*$. The best algorithm known for this problem is the number field sieve [22] which has a *subexponential* expected running time: $\exp((1.923 + o(1))(\log p)^{1/3}(\log\log p)^{2/3})$.

To circumvent this attack, the prime p should be chosen to be sufficiently large. As of 2001, a prime p of bitlength 1024 bits is recommended for medium-term security. For long-term security, larger moduli should be used. As a consequence of this, the implementation of discrete log cryptosystems using the group $\mathbb{Z}_p^*$ is infeasible or impractical in some constrained computational environments; for example, smart cards and hand-held wireless devices such as cellular telephones and pagers [4].

Over the years, a variety of groups have been proposed for use in discrete log cryptosystems. These include: (i) the multiplicative group of a finite field of characteristic 2; (ii) a proper subgroup of the multiplicative group of a finite field [23]; (iii) the group of units of $\mathbb{Z}_n$, n being a composite integer [18]; (iv) the group of points on an elliptic curve defined over a finite field [12, 19]; (v) the Jacobian of a hyperelliptic curve defined over a finite field [13]; (vi) the class group of an imaginary quadratic number field [5]; and (vii) the Jacobian of a superelliptic curve defined over a finite field [9].

There are two primary reasons for considering alternative groups. Firstly, the operation in some groups may be easier to implement in software or in hardware than the operation in other groups. Secondly, the discrete logarithm problem in the group may be harder than the discrete logarithm problem in $\mathbb{Z}_p^*$. Consequently, one could use a group G that is smaller than $\mathbb{Z}_p^*$ while maintaining the same level of security. This potentially results in smaller key sizes, bandwidth savings, and faster implementations.

The group $E(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on an elliptic curve E defined over a finite field $\mathbb{F}_q$, is the most attractive of these groups for cryptographic use. The group law (addition of points) can be performed using a few arithmetic operations in the underlying field $\mathbb{F}_q$. By Hasse's Theorem, the order of the group is roughly equal to q. If the largest prime factor of this order is n, then the best algorithm known for the discrete logarithm problem in $E(\mathbb{F}_q)$ (Pollard's rho algorithm [21]) takes $O\left(\sqrt{n}\right)$ steps; *i.e.*, the algorithm takes *fully exponential* time. As a result, one can use an elliptic curve over a finite field $\mathbb{F}_q$ where $q \approx 2^{160}$, and achieve the same level of security as when a group $\mathbb{Z}_p^*$ is used with $p \approx 2^{1024}$ [14].

More generally, one can use the Jacobian of any algebraic curve. Two difficulties arise when using arbitrary curves: (i) how to select a canonical representation from each divisor class? and, (ii) given the canonical representations of two divisor classes, how to efficiently compute the canonical representation of the sum of the two divisor classes? These difficulties can be suitably addressed when the curve used is a hyperelliptic curve defined over a finite field.

If C is a hyperelliptic curve of genus g defined over $\mathbb{F}_q$, then the order of $\mathcal{J}_C(\mathbb{F}_q)$, the Jacobian of C defined over $\mathbb{F}_q$, is roughly q^g. Note that if $g = 1$, then a hyperelliptic curve is an elliptic curve. Jacobian elements can be compactly represented by a pair of polynomials of degree at most g over $\mathbb{F}_q$, and efficiently added using Cantor's algorithm [6]. When g is large, there is a subexponential algorithm due to Adleman, DeMarrais and Huang [1] (see also [20, 8]) for the discrete logarithm problem in $\mathcal{J}(\mathbb{F}_q)$. Moreover, when g is small and ≥ 5, Gaudry's algorithm [10] is faster than Pollard's rho algorithm.

If $g = 2$ or $g = 3$, and n is the largest prime divisor of $\#\mathcal{J}_C(\mathbb{F}_q)$, the best algorithm known takes $O(\sqrt{n})$ steps, *i.e.*, the algorithm takes *fully exponential* time. Consequently, one can use a hyperelliptic curve of genus 2 over a finite field $\mathbb{F}_q$, where $q \approx 2^{80}$, and achieve the same level of security as when an elliptic curve group $E(\mathbb{F}_q)$ is used, where $q \approx 2^{160}$. A potential disadvantage of using curves of genus 2 instead of elliptic curves is that the group operation in the former may be computationally more expensive, even though the underlying finite field is much smaller. However, this disdvantage may be overcome by the faster implementation that may be possible (*e.g.*, in constrained hardware) due to the smaller field size.

We should also mention that hyperelliptic curves have found applications in other areas including primality proving [2], integer factorization [15], and error-correcting codes [3].

In this paper we count the number of isomorphism classes of hyperelliptic curves of genus 2 over a finite field $\mathbb{F}$ with char$\mathbb{F} \neq 2, 5$. The remainder of this paper is organized as follows. §2 provides some basic background and defines the reduced Weierstrass form of a hyperelliptic curve. The number of singular reduced equations is derived in §3. Finally, §4 counts the number of isomorphism classes of hyperelliptic curves.

2 Preliminaries

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field of order q, $\mathbb{F}^* = \mathbb{F}\backslash\{0\}$, and $\overline{\mathbb{F}}$ the algebraic closure of $\mathbb{F}$. $\mathbb{P}^t$ is the t-dimensional projective space over $\overline{\mathbb{F}}$. The discriminant of a polynomial $f \in \mathbb{F}[x]$ is denoted by $D(f)$; *i.e.*, $D(f) = \text{Resultant}(f, f')$, where f' is the derivative of f. We henceforth assume that char$\mathbb{F} \neq 2, 5$.

A *hyperelliptic curve C of genus g over* $\mathbb{F}$ is a projective non-singular irreducible curve of genus g defined over $\mathbb{F}$ for which there exists a map $C \to \mathbb{P}^1$ of degree two. As in [17], we further assume that C has an $\mathbb{F}$-rational point P such that the $\mathbb{F}$-rational function field of C has a nonconstant function whose only pole is a double one at P; such a point P is called a *Weierstrass point*. We denote the set of all hyperelliptic curves of genus g over $\mathbb{F}$ by $\mathfrak{H}_g$.

Two curves in $\mathfrak{H}_g$ are said to be *isomorphic* over $\mathbb{F}$ if they are isomorphic as projective varieties over $\mathbb{F}$. Briefly, two projective varieties V_1, V_2 over $\mathbb{F}$ are isomorphic over $\mathbb{F}$ if there exist morphisms $\phi : V_1 \longrightarrow V_2$, $\psi : V_2 \longrightarrow V_1$ (ϕ ,ψ defined over $\mathbb{F}$), such that $\psi \circ \phi$, $\phi \circ \psi$ are the identity maps on V_1, V_2 respectively (*cf.* [25, Definition, p.17]). The relation of isomorphism over $\mathbb{F}$ is an equivalence relation on $\mathfrak{H}_g$.

If $C_1, C_2 \in \mathfrak{H}_g$ are isomorphic over $\mathbb{F}$, then their $\mathbb{F}$-Jacobians $\mathcal{J}_{C_1}(\mathbb{F})$ and $\mathcal{J}_{C_2}(\mathbb{F})$ are also isomorphic as abelian groups [26, Chapter III, Remark 2.6.1]. Thus, a classification of the isomorphism classes of genus-2 hyperelliptic curves over $\mathbb{F}$ is relevant to hyperelliptic curve cryptography because it is the $\mathbb{F}$-Jacobians of these curves that are used as finite groups in discrete logarithm cryptographic schemes. Note, however, that if $C_1, C_2 \in \mathfrak{H}_g$ are such that $\mathcal{J}_{C_1}(\mathbb{F})$ and $\mathcal{J}_{C_2}(\mathbb{F})$ are isomorphic (as abelian groups), then this does not imply that

C_1 and C_2 are isomorphic (as projective varieties) over $\mathbb{F}$.

A *Weierstrass equation* H of genus g over $\mathbb{F}$ is an equation of the form

$$H/\mathbb{F} \,:\, v^2 + h(u)v = f(u) \tag{1}$$

where $h, g \in \mathbb{F}[u]$, deg $h \leq g$, deg $f = 2g+1$, f is monic, and there are no singular affine points (or, equivalently, $D(4f + h^2) \neq 0$ [17, Theorem 1.7]). It is easily checked that the curve H has a unique point O at infinity; namely, $O = [0,0,1]$ in the homogeneous coordinates $u = x_1/x_0$, $v = x_2/x_0$. Moreover, O is a singular point of multiplicity $2g-1$ and the line at infinity $x_0 = 0$ is tangent to the curve at this point. We denote the set of all Weierstrass equations of genus g over $\mathbb{F}$ by $\mathfrak{W}_g$.

As is well-known (*e.g.*, see [17, Proposition 1.2]), for every hyperelliptic curve $C \in \mathfrak{H}_g$ there exists a Weierstrass equation $H \in \mathfrak{W}_g$ and a birational morphism $C \to H$. Proposition 1 follows from the discussion in [17].

Proposition 1 ([17]). *There is a 1-1 correspondence between isomorphism classes of curves in $\mathfrak{H}_g$ and equivalence classes of Weierstrass equations in $\mathfrak{W}_g$ where $H, H' \in \mathfrak{W}_g$ are said to be equivalent over $\mathbb{F}$ if there exist $\alpha, \beta \in \mathbb{F}$ with $\alpha \neq 0$, and $t \in \mathbb{F}[u]$ with deg $t \leq g$, such that the change of coordinates $(u, v) \mapsto (\alpha^2 u + \beta, \alpha^5 v + t)$ transforms equation H to equation H'.*

Thus to count the number of isomorphism classes in $\mathfrak{H}_g$, it suffices to count the number of equivalence classes in $\mathfrak{W}_g$.

Assume now that $g = 2$, so $h(u) = a_1 u^2 + a_3 u + a_5$, and $f(u) = u^5 + a_2 u^4 + a_4 u^3 + a_6 u^2 + a_8 u + a_{10}$, with all $a_i \in \mathbb{F}$. Then equation (1) defining a hyperelliptic curve H of genus 2 is unique up to a change of coordinates of the form (see [17, Proposition 1.2])

$$(u, v) \mapsto \left(\alpha^2 u + \beta, \alpha^5 v + \alpha^4 \gamma u^2 + \alpha^2 \delta u + \epsilon\right) \tag{2}$$

where $\alpha \in \mathbb{F}^*$, and $\beta, \gamma, \delta, \epsilon \in \mathbb{F}$. By carrying out the change of coordinates (2) in (1) and computing the values for the new coefficients $\overline{a}_i$ corresponding to the formula (1) we obtain

$$\left\{ \begin{array}{rcl}
\alpha \overline{a}_1 & = & a_1 + 2\gamma \\
\alpha^3 \overline{a}_3 & = & a_3 + 2\beta a_1 + 2\delta \\
\alpha^5 \overline{a}_5 & = & a_5 + \beta a_3 + \beta^2 a_1 + 2\epsilon \\
\alpha^2 \overline{a}_2 & = & a_2 - \gamma a_1 - \gamma^2 + 5\beta \\
\alpha^4 \overline{a}_4 & = & a_4 - \gamma a_3 + 4\beta a_2 - (\delta + 2\beta\gamma) a_1 - 2\gamma\delta + 10\beta^2 \\
\alpha^6 \overline{a}_6 & = & a_6 - \gamma a_5 + 3\beta a_4 - (\delta + \beta\gamma) a_3 + 6\beta^2 a_2 \\
 & & -(\epsilon + 2\beta\delta + \beta^2\gamma) a_1 - \delta^2 - 2\gamma\epsilon + 10\beta^3 \\
\alpha^8 \overline{a}_8 & = & a_8 + 2\beta a_6 - \delta a_5 + 3\beta^2 a_4 - (\epsilon + \beta\delta) a_3 + 4\beta^3 a_2 \\
 & & -(\beta^2\delta + 2\beta\epsilon) a_1 - 2\delta\epsilon + 5\beta^4 \\
\alpha^{10} \overline{a}_{10} & = & a_{10} + \beta a_8 + \beta^2 a_6 - \epsilon a_5 + \beta^3 a_4 - \beta\epsilon a_3 + \beta^4 a_2 - \beta^2 \epsilon a_1 \\
 & & -\epsilon^2 + \beta^5.
\end{array} \right. \tag{3}$$

Proposition 2. *Every hyperelliptic curve of genus 2 can be represented by an equation of the form*

$$v^2 = u^5 + a_4 u^3 + a_6 u^2 + a_8 u + a_{10}. \tag{4}$$

If $H/\mathbb{F}$, $\overline{H}/\mathbb{F}$ are two genus-2 non-singular hyperelliptic curves given by

$$\begin{aligned} H &: v^2 = u^5 + a_4 u^3 + a_6 u^2 + a_8 u + a_{10}, \\ \overline{H} &: v^2 = u^5 + \overline{a}_4 u^3 + \overline{a}_6 u^2 + \overline{a}_8 u + \overline{a}_{10}, \end{aligned}$$

then the only changes of coordinates transforming H to $\overline{H}$ are those of the form

$$(u, v) \mapsto (\alpha^2 u, \alpha^5 v), \qquad \alpha \in \mathbb{F}^*, \tag{5}$$

such that,

$$\left\{ \begin{array}{lcl} \alpha^4 \overline{a}_4 & = & a_4 \\ \alpha^6 \overline{a}_6 & = & a_6 \\ \alpha^8 \overline{a}_8 & = & a_8 \\ \alpha^{10} \overline{a}_{10} & = & a_{10}. \end{array} \right. \tag{6}$$

Proof. Letting $\beta = -a_2/5 - a_1^2/20$, $\gamma = -a_1/2$, $\delta = -a_3/2 + a_1 a_2/5 + a_1^3/20$, and $\epsilon = -a_5/2 + a_3 a_2/10 + a_3 a_1^2/40 - a_1 a_2^2/50 - a_2 a_1^3/100 - a_1^5/800$ in (2), we obtain $\overline{a}_1 = \overline{a}_2 = \overline{a}_3 = \overline{a}_5 = 0$. Moreover, if $a_i = \overline{a}_i = 0$ for $i = 1, 2, 3, 5$, then from the first four equations in (3) we deduce $\beta = \gamma = \delta = \epsilon = 0$. $\square$

The *moduli space* $\mathbf{M}_g$ over an algebraically closed field $\mathbb{K}$ is an irreducible quasi-projective variety over $\mathbb{K}$ whose elements are in 1-1 correspondence with the isomorphism classes of genus-g curves over $\mathbb{K}$. It is known [11, p.347] that the dimension of M_g over $\mathbb{K}$ is 1 if $g = 1$ and $3g - 3$ for $g \geq 2$. Moreover, the isomorphism classes of genus-g hyperelliptic curves over $\mathbb{K}$ correspond to an irreducible subvariety $\mathbf{H}_g$ of $\mathbf{M}_g$ of dimension $2g - 1$. These results suggest that the number of isomorphism classes of genus-g hyperelliptic curves over a finite field $\mathbb{F}$ of order q is on the order of q^{2g-1}. This has been confirmed for the elliptic curve case:

Theorem 3 ([24]). *Let $\left(\frac{a}{b}\right)$ denote the usual Jacobi symbol. We also define*

$$\left(\frac{a}{2}\right) = \left\{ \begin{array}{rl} 1 & \text{if } a \equiv \pm 1 \pmod 8 \\ 0 & \text{if } a \equiv 0 \pmod 2 \\ -1 & \text{if } a \equiv \pm 3 \pmod 8. \end{array} \right.$$

The number of isomorphism classes of elliptic curves over $\mathbb{F}_q$ is $2q + 3 + \left(\frac{-4}{q}\right) + 2\left(\frac{-3}{q}\right)$.

One would expect then that the number of isomorphism classes of genus-2 hyperelliptic curves over $\mathbb{F}_q$ is on the order of q^3. The remainder of this paper derives an exact count in the case when the characteristic of $\mathbb{F}$ is different from 2 and 5 (see Theorem 5).

3 Number of singular reduced equations

We denote by $|X|$ the cardinality of a finite set X. $\mathbb{F}^{(2)} = \{\alpha^2 : \alpha \in \mathbb{F}\}$ denotes the set of squares in $\mathbb{F}$.

Theorem 4. *Let* $V = \{g(u) = u^5 + au^3 + bu^2 + cu + d \in \mathbb{F}[u] : D(g) = 0\}$*. Then* $|V| = q^3$*.*

Proof. Let $g(u) = u^5 + au^3 + bu^2 + cu + d \in \mathbb{F}[u]$ with $D(g) = 0$. Then $g(u)$ has a multiple root $\alpha \in \overline{\mathbb{F}}$. Hence we have one of the following two factorizations of $g(u)$ in $\mathbb{F}[u]$:

(i) If $\alpha \in \mathbb{F}$, then $g(u) = (u-\alpha)^2(u^3 + 2\alpha u^2 + \beta u + \gamma)$, with $\beta, \gamma \in \mathbb{F}$.

(ii) If $\alpha \notin \mathbb{F}$, then $g(u) = (u^2 + \lambda u + \mu)^2(u - 2\lambda)$, with $(\lambda, \mu) \in \mathbb{F}^2 \backslash S$, $S = \{(\lambda, \mu) \in \mathbb{F}^2 : \lambda^2 - 4\mu \in \mathbb{F}^{(2)}\}$ (i.e., $(u^2 + \lambda u + \mu)$ is irreducible over $\mathbb{F}$).

Define the maps

$$\tag{7} \begin{cases} \varphi\colon \mathbb{F}^3 \to V, & \varphi(\alpha, \beta, \gamma) = (u-\alpha)^2(u^3 + 2\alpha u^2 + \beta u + \gamma), \\ \psi\colon \mathbb{F}^2 \backslash S \to V, & \psi(\lambda, \mu) = (u^2 + \lambda u + \mu)^2(u - 2\lambda). \end{cases}$$

As the parametrizations (i) and (ii) are mutually excluding we have

$$|V| = |\operatorname{Im}\varphi| + |\operatorname{Im}\psi|.$$

Now, ψ is clearly injective so $|\operatorname{Im}\psi|$ is equal to the number of monic irreducible quadratics over $\mathbb{F}$, namely $\frac{1}{2}q(q-1)$ [16, Theorem 3.25]. Suppose now that $\varphi(\alpha, \beta, \gamma) = \varphi(\overline{\alpha}, \overline{\beta}, \overline{\gamma})$, where $(\alpha, \beta, \gamma) \neq (\overline{\alpha}, \overline{\beta}, \overline{\gamma})$. That is $g(u) = \overline{g}(u)$, where $g(u) = (u-\alpha)^2(u^3 + 2\alpha u^2 + \beta u + \gamma)$ and $\overline{g}(u) = (u-\overline{\alpha})^2(u^3 + 2\overline{\alpha}u^2 + \overline{\beta}u + \overline{\gamma})$. We must have $\alpha \neq \overline{\alpha}$ since if $\alpha = \overline{\alpha}$ then $(u^3 + 2\alpha u^2 + \beta u + \gamma) = (u^3 + 2\overline{\alpha}u^2 + \overline{\beta}u + \overline{\gamma})$ whence $\beta = \overline{\beta}$ and $\gamma = \overline{\gamma}$. Hence

$$\tag{8} g(u) = \overline{g}(u) = (u-\alpha)^2(u-\overline{\alpha})^2(u-\delta), \text{ where } \delta = -2\alpha - 2\overline{\alpha}.$$

For such $g(u)$, $(\alpha, \beta, \gamma) \in \mathbb{F}^3$ such that $\varphi(\alpha, \beta, \gamma) = g(u)$ is uniquely determined by $\beta = \overline{\alpha}^2 - 2\overline{\alpha}\delta$ and $\gamma = -\delta\overline{\alpha}^2$. Similarly, $(\overline{\alpha}, \overline{\beta}, \overline{\gamma}) \in \mathbb{F}^3$ such that $\varphi(\overline{\alpha}, \overline{\beta}, \overline{\gamma}) = g(u)$ is uniquely determined by $\overline{\beta} = \alpha^2 - 2\alpha\delta$ and $\overline{\gamma} = -\delta\alpha^2$. Now, the only $g(u) \in V$ which are the images under φ of more than one triple $(\alpha, \beta, \gamma) \in \mathbb{F}^3$ are precisely those $g(u)$ of the form (8) where $\alpha \neq \overline{\alpha}$. Moreover, for each such $g(u)$, there are precisely two triples in $\mathbb{F}^3$ which are mapped by φ to $g(u)$, namely (α, β, γ) and $(\overline{\alpha}, \overline{\beta}, \overline{\gamma})$. Since there are $\frac{1}{2}q(q-1)$ polynomials of the form (8), it follows that $|\operatorname{Im}\varphi| = q^3 - \frac{1}{2}q(q-1)$.

Finally, we have $|V| = |\operatorname{Im}\varphi| + |\operatorname{Im}\psi| = q^3$. □

4 Number of isomorphism classes

Let $\mathcal{H}$ be the set of equations of the form (4) satisfying $D(u^5+a_4u^3+a_6u^2+a_8u+a_{10}) \neq 0$. Let G be the group of transformations of the form $(u,v) \mapsto (\alpha^2 u, \alpha^5 v)$, $\alpha \in \mathbb{F}^*$ as in (5). As we proved in Proposition 2, every genus-2 hyperelliptic curve over $\mathbb{F}$ can be represented by an equation in $\mathcal{H}$. Moreover, G acts on $\mathcal{H}$ in a natural way so that $\mathcal{H}/G$ is the set of isomorphism classes of such curves.

Theorem 5. *The number of isomorphism classes of genus-2 hyperelliptic curves over $\mathbb{F}_q$ is $|\mathcal{H}/G| = 2q^3 + r(q)$, where $r(q)$ is given in the following table:*

$r(q)$	$q \equiv 1 (\mathrm{mod}\, 8)$	$q \not\equiv 1 (\mathrm{mod}\, 8), q \equiv 1 (\mathrm{mod}\, 4)$	$q \not\equiv 1 (\mathrm{mod}\, 4)$
$q \equiv 1 (\mathrm{mod}\, 5)$	$2q+10$	$2q+6$	8
$q \not\equiv 1 (\mathrm{mod}\, 5)$	$2q+2$	$2q-2$	0

Proof. Let $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3, \mathcal{H}_4$ be the subsets in $\mathcal{H}$ defined as follows:

$$\begin{aligned}
\mathcal{H}_1 &= \{H \in \mathcal{H} : a_4 = a_6 = a_8 = 0, a_{10} \neq 0\}, \\
\mathcal{H}_2 &= \{H \in \mathcal{H} : a_4 = a_6 = a_{10} = 0, a_8 \neq 0\}, \\
\mathcal{H}_3 &= \{H \in \mathcal{H} : a_6 = a_{10} = 0, a_4 \neq 0, a_8 \neq 0\}, \\
\mathcal{H}_4 &= \mathcal{H} \backslash (\mathcal{H}_1 \cup \mathcal{H}_2 \cup \mathcal{H}_3).
\end{aligned}$$

Then, we have $\mathcal{H} = \mathcal{H}_1 \cup \mathcal{H}_2 \cup \mathcal{H}_3 \cup \mathcal{H}_4$ (disjoint union). From Theorem 4, we readily obtain $|\mathcal{H}| = q^4 - q^3$, $|\mathcal{H}_1| = |\mathcal{H}_2| = q-1$, and $|\mathcal{H}_3| = (q-1)(q-2)$. Hence $|\mathcal{H}_4| = |\mathcal{H}| - |\mathcal{H}_1 \cup \mathcal{H}_2 \cup \mathcal{H}_3| = q(q-1)^2(q+1)$. We remark that $G \cong \mathbb{F}^*$; hence $|G| = q-1$. Moreover, the curves in each subset $\mathcal{H}_i$ have the same isotropy group in G; let us denote it by G_i, for $i = 1,2,3,4$. By using the formulas (6), a simple calculation shows that

$$G_1 = \left\{\alpha \in \mathbb{F}^* : \alpha^{10}{=}1\right\}, \quad G_2 = \left\{\alpha \in \mathbb{F}^* : \alpha^{8}{=}1\right\},$$

$$G_3 = \left\{\alpha \in \mathbb{F}^* : \alpha^{4}{=}1\right\}, \quad G_4 = \left\{\alpha \in \mathbb{F}^* : \alpha^{2}{=}1\right\}.$$

Since $\mathbb{F}^*$ is a cyclic group of order $q-1$ and q is odd, it follows that $|G_4| = 2$,

$$|G_1| = \begin{cases} 10, & \text{if } q \equiv 1 \pmod 5 \\ 2, & \text{if } q \not\equiv 1 \pmod 5, \end{cases}$$

$$|G_2| = \begin{cases} 8, & \text{if } q \equiv 1 \pmod 8 \\ 4, & \text{if } q \not\equiv 1 \pmod 8 \text{ and } q \equiv 1 \pmod 4 \\ 2, & \text{if } q \not\equiv 1 \pmod 4, \end{cases}$$

$$|G_3| = \begin{cases} 4, & \text{if } q \equiv 1 \pmod 4 \\ 2, & \text{if } q \not\equiv 1 \pmod 4. \end{cases}$$

Let $(G : G_i)$ denote the index of the subgroup G_i in G. The result now follows because

$$\begin{aligned}|\mathcal{H}/G| &= \frac{|\mathcal{H}_1|}{(G:G_1)} + \frac{|\mathcal{H}_2|}{(G:G_2)} + \frac{|\mathcal{H}_3|}{(G:G_3)} + \frac{|\mathcal{H}_4|}{(G:G_4)} \\ &= \frac{|\mathcal{H}_1||G_1|}{|G|} + \frac{|\mathcal{H}_2||G_2|}{|G|} + \frac{|\mathcal{H}_3||G_3|}{|G|} + \frac{|\mathcal{H}_4||G_4|}{|G|} \\ &= 2q^3 - 2q + |G_1| + |G_2| + (q-2)|G_3|.\end{aligned}$$

□

Acknowledgements

We are grateful to Y. Choie and D. Yun for pointing out a flaw in an earlier version of Theorem 5.

References

[1] L. Adleman, J. DeMarrais and M. Huang, *A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields*, Algorithmic Number Theory, LNCS **877** (1994), 28–40, Springer-Verlag, Berlin.

[2] L. Adleman and M. Huang, *Primality Testing and Abelian Varieties Over Finite Fields*, LNM **1512** (1992), Springer-Verlag, Berlin.

[3] D. Le Brigand, *Decoding of codes on hyperelliptic curves*, Eurocode'90, LNCS **514** (1991), 126–134, Springer-Verlag, Berlin.

[4] M. Brown, D. Cheung, D. Hankerson, J. Hernandez, M. Kirkup and A. Menezes, *PGP in constrained wireless devices*, Proceedings of the Ninth USENIX Security Symposium, 247–261, 2000.

[5] J. Buchmann and H. Williams, *A key-exchange system based on imaginary quadratic fields*, J. Cryptology **1** (1988), 107–118.

[6] D. Cantor, *Computing in the jacobian of a hyperelliptic curve*, Math. Comp. **48** (1987), 95–101.

[7] W. Diffie and M. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory **22** (1976), 644–654.

[8] A. Enge and P. Gaudry, *A general framework for subexponential discrete logarithm algorithms*, Acta Arithmetica, to appear.

[9] S. Galbraith, S. Paulus and N. Smart, *Arithmetic of superelliptic curves*, Math. Comp. **71** (2002), 393-405.

[10] P. Gaudry, *An algorithm for solving the discrete log problem on hyperelliptic curves*, Advances in Cryptology – Eurocrypt 2000, LNCS **1807** (2000), 19–34, Springer-Verlag, Berlin.

[11] R. Hartshorne, *Algebraic Geometry*, Springer Verlag, New York, 1977.

[12] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), 203–209.

[13] — , *Hyperelliptic cryptosystems*, J. Cryptology **1** (1989), 139–150.

[14] A. Lenstra and E. Verheul, *Selecting cryptographic key sizes*, Proceedings of PKC 2000, LNCS **1751** (2000), 446–465, Springer-Verlag, Berlin.

[15] H.W. Lenstra, J. Pila and C. Pomerance, *A hyperelliptic smoothness test. I*, R. Soc. Philos. Trans. Ser. A Math. Phys. Eng. Sci. **345** (1993), 397–408.

[16] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1994.

[17] P. Lockhart, *On the discriminant of a hyperelliptic curve*, Trans. Amer. Math. Soc. **342**, 2 (1994), 729–752

[18] K. McCurley, *A key distribution system equivalent to factoring*, J. Cryptology **1** (1988), 95–105.

[19] V. Miller, *Uses of elliptic curves in cryptography*, Advances in Cryptology-CRYPTO'85, LNCS **218** (1986), 417–426, Springer-Verlag, Berlin.

[20] V. Müller, A. Stein and C. Thiel, *Computing discrete logarithms in real quadratic congruence function fields of large genus*, Math. Comp. **68** (1999), 807–822.

[21] J. Pollard, *Monte Carlo methods for index computation mod p*, Math. Comp. **32** (1978), 918–924.

[22] O. Schirokauer, D. Weber and T. Denny, *Discrete logarithms: the effectiveness of the index calculus method*, Algorithmic Number Theory, LNCS **1122** (1996), 337–361, Springer-Verlag, Berlin.

[23] C. Schnorr, *Efficient signature generation by smart cards*, J. Cryptology **4** (1991), 161–174.

[24] R Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A **46** (1987), 183–211.

[25] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[26] — , *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.