Reprinted from JOURNAL OF COMBINATORIAL THEORY, Series A
All Rights Reserved by Academic Press, New York and London

Vol. 46, No. 2, November 1987
Printed in Belgium

Nonsingular Plane Cubic Curves over Finite Fields

RENÉ SCHOOF

Mathematical Sciences Research Institute,
1000 Centennial Drive, Berkeley, California 94720

Communicated by the Managing Editors

Received August 28, 1986

We determine the number of projectively inequivalent nonsingular plane cubic curves over a finite field $\mathbb{F}_q$ with a fixed number of points defined over $\mathbb{F}_q$. We count these curves by counting elliptic curves over $\mathbb{F}_q$ together with a rational point which is annihilated by 3, up to a certain equivalence relation. © 1987 Academic Press, Inc.

1. INTRODUCTION

We give a complete answer to the following question:

(1.1) QUESTION. Given a finite field $\mathbb{F}_q$ and an integer $N \geqslant 0$; how many projectively inequivalent nonsingular plane projective cubic curves are there over $\mathbb{F}_q$ that have exactly N points defined over $\mathbb{F}_q$?

Here $\mathbb{F}_q$ denotes a finite field with q elements. Two plane curves are said to be projectively equivalent if there is a projective transformation of the projective $\mathbb{F}_q$-plane mapping the equation of one curve to the equation of the other; see Hirschfeld [12].

This question has been studied from the point of view of combinatorics. Partial answers have been obtained [1, 4–6]. Oddly enough, the matter had essentially been settled by Max Deuring in 1941. In his paper [8] he determined which rings occur as rings of endomorphisms of elliptic curves defined over a finite field. From this he deduced how many isomorphism classes of elliptic curves over a finite field there are in a fixed isogeny class, which implies a good deal of the answer to Question (1.1).

In this paper we explain how to obtain an answer to Question (1.1) from Deuring's results. There are two complications: there is a difference between the notions of projective equivalence of curves in the sense of Hirschfeld and isomorphism of abelian varieties in the sense of algebraic geometry; we overcome this difficulty by studying the 3-torsion points on

0097-3165/87 $3.00

elliptic curves over finite fields. The second complication is the fact that Deuring considers two elliptic curves to be isomorphic over $\mathbb{F}_q$ if they are, in our sense, only isomorphic over $\bar{\mathbb{F}}_q$, the algebraic closure of $\mathbb{F}_q$. For this reason we will consult Waterhouse's 1969 thesis [19] rather than Deuring's paper.

Before we state the main result we introduce some notation: for every $\Delta \in \mathbb{Z}_{<0}$ with $\Delta \equiv 0$ or $1 \pmod 4$ we denote by $H(\Delta)$ the *Kronecker class number* of Δ; the definition of the Kronecker class number is given in Section 2 and a small table of these numbers is given in Section 6. The *Jacobi symbol* is denoted by $\left(\frac{x}{p}\right)$ or (x/p) and is defined as follows: for $x \in \mathbb{Z}$ and p and odd prime

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{if } x \equiv 0 \pmod p; \\ 1 & \text{if } x \text{ is a nonzero square } \pmod p; \\ -1 & \text{if } x \text{ is not a square } \pmod p. \end{cases}$$

For every $x \in \mathbb{Z}$ we define

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

The main result is the following:

Let $\mathbb{F}_q$ be a finite field of characteristic p. Let $M(t)$ denote the number of projectively inequivalent plane cubic curves over $\mathbb{F}_q$ with exactly $q+1-t$ points defined over $\mathbb{F}_q$. We have that

$$M(t) = N(t) + N_3(t) + 3N_{3\times 3}(t) - \varepsilon(t),$$

where

$$\begin{aligned} N(t) &= H(t^2-4q) && \text{if } t^2 < 4q \text{ and } p \nmid t; \\ &= H(-4p) && \text{if } t = 0, \\ &= 1 && \text{if } p = 2 \text{ and } t^2 = 2q, \\ &= 1 && \text{if } p = 3 \text{ and } t^2 = 3q \end{aligned} \Bigg\} \text{ and if } q \text{ is not a square;}$$

$$\left.\begin{aligned} &= \frac{1}{12}\left(p+6-4\left(\frac{-3}{p}\right)-3\left(\frac{-4}{p}\right)\right) && \text{if } t^2 = 4q \\ &= 1-\left(\frac{-3}{p}\right) && \text{if } t^2 = q \\ &= 1-\left(\frac{-4}{p}\right) && \text{if } t = 0 \end{aligned}\right\} \text{ and if } q \text{ is a square;}$$

$$= 0 \qquad \text{otherwise;}$$

$$N_3(t) = N(t) \quad \text{if} \quad t \equiv q+1 \pmod 3;$$
$$= 0 \quad \text{otherwise;}$$
$$N_{3\times 3}(t) = H\left(\frac{t^2-4q}{9}\right) \quad \text{if} \quad q \equiv 1 \pmod 3,\ p \nmid t \text{ and } t \equiv q+1 \pmod 9;$$
$$= N(t) \quad \text{if} \quad q \text{ is a square, } p \neq 3 \text{ and } t = 2\left(\frac{\sqrt{q}}{3}\right)\sqrt{q};$$
$$= 0 \quad \text{otherwise;}$$
$$\varepsilon(t) = 2 \quad \text{if} \quad (t = t_0 \text{ or } t = t_1) \text{ and } t_0 \neq t_1;$$
$$= 3 \quad \text{if} \quad t = t_0 = t_1 \text{ and } p = 2;$$
$$= 4 \quad \text{if} \quad t = t_0 = t_1 \text{ and } p \neq 2;$$
$$= 0 \quad \text{otherwise.}$$

The numbers t_0 and t_1 are defined as follows:

t_0 is only defined if $q \equiv 1 \pmod 3$:

$$t_0 = \text{the unique solution } t \in \mathbb{Z} \text{ to}$$
$$\left\{\begin{array}{l} t \equiv q+1 \pmod 9 \\ p \nmid t \\ t^2+3x^2 = 4q \quad \text{for some } x \in \mathbb{Z} \end{array}\right\} \quad \text{if} \quad p \equiv 1 \pmod 3;$$
$$= 2\left(\frac{\sqrt{q}}{3}\right)\sqrt{q} \quad \text{if} \quad p \not\equiv 1 \pmod 3.$$

t_1 is only defined if $q \equiv 1$ or $4 \pmod{12}$:

$$t_1 = \text{the unique solution } t \in \mathbb{Z} \text{ to}$$
$$\left\{\begin{array}{l} t \equiv q+1 \pmod 9 \\ p \nmid t \\ t^2+4x^2 = 4q \quad \text{for some } x \in \mathbb{Z} \end{array}\right\} \quad \text{if} \quad p \equiv 1 \pmod 4;$$
$$= 2\left(\frac{\sqrt{q}}{3}\right)\sqrt{q} \quad \text{if} \quad p \not\equiv 1 \pmod 4.$$

The paper is organized as follows: In Section 2 we give the definitions of class numbers of complex quadratic orders, in terms of which the main result is formulated. In Section 3 we give some definitions and facts concerning elliptic curves over finite fields; for the proofs we usually refer to the literature. In Section 4 we compute the number of isomorphism classes of elliptic curves over a finite fields in a fixed isogeny class. For most of the

proofs we refer to the thesis of Waterhouse [19]. In this section we also compute the number of elliptic curves in a fixed isogeny class that have their n-torsion points rational over the field of definition. For the definitions of all this see Section 3.

In Section 5 we obtain a one-to-one correspondence between equivalence classes of nonsingular plane cubic curves in the sense of Hirschfeld and elliptic curves furnished with an embedding in the projective plane modulo a certain equivalence relation. In this section we deduce the main result: a formula for the number of projectively inequivalent nonsingular plane cubics over $\mathbb{F}_q$ with a fixed number of $\mathbb{F}_q$-rational points.

By counting $\mathbb{F}_q$-rational points on the modular curves $X(1)$ and $X_1(3)$ we obtain a formula for the total number of projectively inequivalent nonsingular cubic curves over $\mathbb{F}_q$; our formula for the total number of curves agrees with the one given by Hirschfeld [12, p. 315] column N.

Finally, in Section 6, we give a table of Kronecker class numbers and as an illustration we count how many projectively inequivalent plane cubic curves there are over $\mathbb{F}_q$ with a given number of points over $\mathbb{F}_q$ for some small values of q.

We will use the following notations: for every $n \in \mathbb{Z}$ and for every abelian group A we denote by $A[n]$ its n-torsion subgroup: $A[n] = \{a \in A: na = 0\}$. By μ_n we denote the group of nth roots of unity in $\mathbb{C}$. By ζ we denote a primitive 3rd root of unity and by i a primitive 4th root of unity.

2. Class Numbers

In this section we give the definitions of class numbers of complex quadratic orders and of class numbers of the sets of binary quadratic forms with discriminant $\Delta \in \mathbb{Z}_{<0}$. Complex quadratic orders occur as rings of endomorphisms of elliptic curves over finite fields. The set of isomorphism classes of elliptic curves over $\mathbb{F}_q$ which have a fixed complex quadratic order $\mathcal{O}$ as their ring of endomorphisms is a (usually principal) homogeneous space over the class group of $\mathcal{O}$. The study of binary quadratic forms is very old; it was initiated by Gauss [10].

Let $\Delta \in \mathbb{Z}_{<0}$ with $\Delta \equiv 0$ or $1 \pmod 4$; by

$$B(\Delta) = \{aX^2 + bXY + cY^2 \in \mathbb{Z}[X, Y]: a > 0 \text{ and } b^2 - 4ac = \Delta\}$$

we denote the set of positive definite binary quadratic forms of discriminant Δ and by

$$b(\Delta) = \{aX^2 + bXY + cY^2 \in B(\Delta): \gcd(a, b, c) = 1\}$$

we denote the primitive forms of discriminant Δ. The group $SL_2(\mathbb{Z})$ acts on $B(\Delta)$ as follows: let $f = aX^2 + bXY + cY^2 \in B(\Delta)$ and let $\sigma = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$; we let

$$f \circ \sigma = a(pX + qY)^2 + b(pX + qY)(rX + sY) + c(rX + sY)^2;$$

one checks easily that $f \circ \sigma \in B(\Delta)$ and that $SL_2(\mathbb{Z})$ respects the subset of primitive forms $b(\Delta)$.

It can be shown that there are only finitely many $SL_2(\mathbb{Z})$-orbits in $B(\Delta)$.

(2.1) DEFINITION. We let $\mathrm{CL}(\Delta) = B(\Delta)/SL_2(\mathbb{Z})$, the set of $SL_2(\mathbb{Z})$-orbits in $B(\Delta)$; similarly we let $\mathrm{Cl}(\Delta) = b(\Delta)/SL_2(\mathbb{Z})$. By $H(\Delta)$, the Kronecker class number, we denote the cardinality of $\mathrm{CL}(\Delta)$ and by $h(\Delta)$, the (ordinary) class number we denote the cardinality of $\mathrm{Cl}(\Delta)$.

(2.2) PROPOSITION. *Let $\Delta \in \mathbb{Z}_{<0}$ congruent to* 0 *or* 1 (mod 4). *We have*

$$\sum_d h\left(\frac{\Delta}{d^2}\right) = H(\Delta),$$

where d runs over $d \in \mathbb{Z}_{>0}$ for which $d^2 \mid \Delta$ and $\Delta/d^2 \equiv 0$ or 1 (mod 4).

Proof. Sort the quadratic forms $aX^2 + bXY + cY^2$ in $B(\Delta)$ according to $\gcd(a, b, c)$. We have a one-to-one correspondence between the sets $\{f \in B(\Delta) : \gcd(a, b, c) = d\}/SL_2(\mathbb{Z})$ and $\{f \in B(\Delta/d^2) : \gcd(a, b, c) = 1\}/SL_2(\mathbb{Z})$. This proves the proposition.

A complex quadratic order $\mathcal{O}$ is a subring of finite index in the ring of integers in a complex quadratic number field. There is upto conjugation a unique embedding $\mathcal{O} \subsetneq \mathbb{C}$. For $\alpha \in \mathcal{O}$ we let $T(\alpha) = \alpha + \bar{\alpha}$ and $N(\alpha) = \alpha\bar{\alpha}$; here $\bar{\alpha}$ denotes the complex conjugate of α. Both $T(\alpha)$ and $N(\alpha)$ are elements in $\mathbb{Z}$. By $\Delta(\mathcal{O})$ we denote the discriminant of $\mathcal{O}$; see [2].

Let K be a complex quadratic number field. By $\mathcal{O}_{\max}$ we denote the ring of integers in K. For every $k \in \mathbb{Z}_{>0}$, the ring $\mathcal{O}_{\max}$ has precisely one subring $\mathcal{O}$ of index k. The discriminant of this order equals $\Delta(\mathcal{O}_{\max})\, k^2$. This implies that complex quadratic orders are characterized by their discriminants: by $\mathcal{O}(\Delta)$ we shall denote the complex quadratic order of discriminant Δ. If α is an algebraic number for which $\mathcal{O} = \mathbb{Z}[\alpha]$ is a complex quadratic order then $\Delta(\mathcal{O})$ equals the discriminant of the minimum polynomial of α. For more facts concerning complex quadratic orders see [2].

(2.3) DEFINITION. Let $\mathcal{O}$ be a complex quadratic order; by $\mathrm{Cl}(\mathcal{O})$ we denote the class group of $\mathcal{O}$: it is the group of invertible $\mathcal{O}$-ideals modulo invertible principal $\mathcal{O}$-ideals. The class group is a finite group and its order, the class number of $\mathcal{O}$, will be denoted by $h(\mathcal{O})$.

We have in fact that $h(\mathcal{O}) = h(\Delta(\mathcal{O}))$ in the sense of Definition (2.1).

(2.4) PROPOSITION. *Let $\mathcal{O}$ be a complex quadratic order. We have that*

$$\sum_{\mathcal{O} \subset \mathcal{O}' \subset \mathcal{O}_{\max}} h(\mathcal{O}') = H(\Delta(\mathcal{O})).$$

Proof. For every order $\mathcal{O}'$ with $\mathcal{O} \subset \mathcal{O}' \subset \mathcal{O}_{\max}$ we have that $\Delta(\mathcal{O}') = \Delta(\mathcal{O})/[\mathcal{O}':\mathcal{O}]^2$. Since $h(\mathcal{O}') = h(\Delta(\mathcal{O}'))$ the result follows immediately from Proposition (2.2).

The definitions of $H(\Delta)$ and $h(\Delta)$ given above are not very suitable for computation; below we give another, less natural, definition, which is suitable for actual computation.

(2.5) PROPOSITION. *Let $\Delta \in \mathbb{Z}_{<0}$ congruent to 0 or 1 (mod 4). Put*

$$\tilde{B}(\Delta) = \{(a, b, c) \in \mathbb{Z}^3 : a > 0,\ b^2 - 4ac = \Delta,\ |b| \leqslant a \leqslant c,$$
$$\text{and } b \geqslant 0 \text{ whenever } a = |b| \text{ or } a = c\};$$
$$\tilde{b}(\Delta) = \{(a, b, c) \in \tilde{B}(\Delta) : \gcd(a, b, c) = 1\}.$$

We have that

$$H(\Delta) = \#\tilde{B}(\Delta) \qquad \text{and} \qquad h(\Delta) = \#\tilde{b}(\Delta).$$

Proof. In every $SL_2(\mathbb{Z})$-orbit of $B(\Delta)$ or $b(\Delta)$ there exists one and only one quadratic form $aX^2 + bXY + cY^2$ for which $|b| \leqslant a \leqslant c$, and $b \geqslant 0$ whenever $a = |b|$ or $a = c$. Such a form is called reduced. Identifying $aX^2 + bXY + cY^2$ with $(a, b, c) \in \mathbb{Z}^3$ gives the required result.

We see that $(a, b, c) \in \tilde{B}(\Delta)$ implies that $4a^2 \leqslant 4ac = |\Delta| + b^2 \leqslant |\Delta| + a^2$ and hence $a \leqslant \sqrt{|\Delta|/3}$. From this we get at once that $\tilde{B}(\Delta)$ is a finite set. Our answer to Question (1.1) involves the numbers $H(\Delta)$. It should be stressed that $H(\Delta)$ and $h(\Delta)$ should be considered to be easily computable numbers. For a given field $\mathbb{F}_q$ it is much quicker to compute the class numbers $H(t^2 - 4q)$ for $t \in \mathbb{Z}$, $t^2 < 4q$ and apply Theorem (2.5) than to compute all inequivalent cubic curves and count their $\mathbb{F}_q$-rational points like De Groote and Hirschfeld did for $q \leqslant 13$ in [6].

At the end of this paper we give a small table of the numbers $H(\Delta)$ for $|\Delta| \leqslant 200$. This table can be computed by hand in a few minutes and suffices to give an answer to Question (1.1) for all fields $\mathbb{F}_q$ with $q \leqslant 49$. Larger tables of $h(\Delta)$ and $H(\Delta)$ have been computed; for instance Buell computed $h(\Delta)$ for all Δ with $|\Delta| < 25 \times 10^6$, see [3]. Using Proposition (2.2) one obtains easily the numbers $H(\Delta)$ from this table.

3. Elliptic Curves over Finite Fields

In this section we state some basic properties of elliptic curves over finite fields. For proofs, more properties and references to the literature see [17].

(3.1) Definition. Let K be a field; an *elliptic curve E over K* is a projective nonsingular algebraic curve of genus one defined over K furnished with a point 0 on E which is defined over K.

Let $\bar{K}$ denote an algebraic closure of K; by $E(\bar{K})$ we denote the set of points on E defined over $\bar{K}$. This set is in a natural geometric way an abelian group with 0 as the zero-element. The set $E(K)$ of points on E that are defined over K is a subgroup of $E(\bar{K})$; see [17].

(3.2) Definition. A *morphism* of elliptic curves over K: $E_1 \to^f E_2$ is an algebraic map defined over K that respects the group law; in particular $f(0_1)=0_2$. An isomorphism is a morphism that has a two-sided inverse. For any elliptic curve E over K the morphisms $E \to^f E$ form a ring, the *ring of K-endomorphisms of E*; this ring will be denoted by $\mathrm{End}_K(E)$. The units of this ring are called the K-automorphisms of E. We will denote the group of K-automorphisms by $\mathrm{Aut}_K(E)$.

Every elliptic curve E over K is isomorphic to a curve given by an equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \quad (a_i \in K) \qquad (1)$$

in $\mathbb{P}^2_K$; the point 0 is the point at infinity (0:1:0). This follows from the Riemann–Roch theorem.

We have the usual formulaire

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2,\\
b_4 &= a_1a_3 + 2a_4,\\
b_6 &= a_3^2 + 4a_6,\\
b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2,\\
c_4 &= b_2^2 - 24b_4,\\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6,\\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\
j &= c_4^3/\Delta.
\end{aligned}$$

A curve given by Eq. (1) is an elliptic curve if and only if the discriminant Δ is not zero. The j-invariant of an elliptic curve E depends only on its isomorphism class: two elliptic curves over K have the same

j-invariant if and only if they are isomorphic over $\bar{K}$. This is in general not true over K: there may be non-isomorphic curves over K that are isomorphic over $\bar{K}$.

Two values of j deserve special attention: they are the values 0 and 1728. The elliptic curves whose j-invariants assume these values correspond to the harmonic curves if $j = 1728$ and to the equianharmonic curves if $j = 0$ in the sense of Hirschfeld [12]. If the characteristic of K is 2 or 3 we have that $0 = 1728$ and the elliptic curves over K with j-invariants equal to $0 = 1728$ correspond to the superharmonic curves in Hirschfeld's book. It is easy to write down an equation of a curve with j-invariant equal to 0 or 1728. If $\mathrm{char}(K) \neq 3$ the curve given by $Y^2 - Y = X^3$ has j-invariant equal to 0 and if $\mathrm{char}(K) \neq 2$ the curve given by the equation $Y^2 = X^3 - X$ has j-invariant equal to 1728.

Next we restrict ourselves to elliptic curves over finite fields. Let $\mathbb{F}_q$ be a finite field with q elements and let $p = \mathrm{char}(\mathbb{F}_q)$. By $\mathbb{Q}_{\infty,p}$ we denote the unique quaternion algebra over $\mathbb{Q}$ which is only ramified at p and ∞. The maximal orders in $\mathbb{Q}_{\infty,p}$ are non-commutative rings of rank four over $\mathbb{Z}$; see [8, 9].

Let E be an elliptic curve over $\mathbb{F}_q$. The rings $\mathrm{End}_{\mathbb{F}_q}(E)$ and $\mathrm{End}_{\bar{\mathbb{F}}_q}(E)$ are either complex quadratic orders or maximal orders in $\mathbb{Q}_{\infty,p}$. It may happen that $\mathrm{End}_{\mathbb{F}_q}(E)$ is complex quadratic and $\mathrm{End}_{\bar{\mathbb{F}}_q}(E)$ is not. We define a norm and a trace on $\mathrm{End}_{\bar{\mathbb{F}}_q}(E)$ as follows: let $\alpha \in \mathrm{End}_{\bar{\mathbb{F}}_q}(E)$; either $\alpha \in \mathbb{Z}$ or $\mathbb{Z}[\alpha]$ is a complex quadratic order; we choose an embedding of $\mathbb{Z}[\alpha]$ in $\mathbb{C}$ and we let $T(\alpha) = \alpha + \bar{\alpha}$ and $N(\alpha) = \alpha\bar{\alpha}$; both $T(\alpha)$ and $N(\alpha)$ are in $\mathbb{Z}$.

The elliptic curves E with j-invariant equal to 0 or 1728 are special: the curves E with $j = 0$ have $\mathbb{Z}[\zeta]$ as a subring of $\mathrm{End}_{\bar{\mathbb{F}}_q}(E)$ and the curves E with $j = 1728$ have $\mathbb{Z}[i]$ as a subring of $\mathrm{End}_{\bar{\mathbb{F}}_q}(E)$. This can easily be seen from the equations given above. In Section 4 we will see that "most" elliptic curves have an endomorphism ring whose group of units is $\{\pm 1\}$. That is, usually $\mathrm{Aut}_{\bar{\mathbb{F}}_q}(E) = \{id, -id\}$; if $\mathbb{Z}[\zeta]$ or $\mathbb{Z}[i]$ is a subring of $\mathrm{End}_{\bar{\mathbb{F}}_q}(E)$, there are more automorphisms and this affects our computations.

(3.3) DEFINITION. An elliptic curve E over $\mathbb{F}_q$ is called *supersingular* if $\mathrm{End}_{\bar{\mathbb{F}}_q}(E)$ is non-commutative.

We see that the supersingularity of a curve E depends only on E over $\bar{\mathbb{F}}_q$, that is, on its j-invariant. We will say that j is supersingular if there is a supersingular curve E with j-invariant equal to j; in this case every elliptic curve with j-invariant equal to j is supersingular. If $p = \mathrm{char}(\mathbb{F}_q)$ equals 2 or 3 the supersingular curves are precisely the ones with their j-invariants equal to $0 = 1728$. In general we have that $j = 0$ is supersingular if and only if $p \not\equiv 1 \pmod 3$ and that $j = 1728$ is supersingular if and only if $p \not\equiv 1 \pmod 4$. If $j = 0$ is not supersingular the curves with j-invariant equal to 0

are precisely the curves with $\mathrm{End}_{\mathbb{F}_q}(E) = \mathbb{Z}[\zeta]$. If $j = 1728$ is not supersingular the curves with j-invariant equal to 1728 are precisely the curves with $\mathrm{End}_{\mathbb{F}_q}(E) = \mathbb{Z}[i]$; see [8, 9, 17].

Next we describe the structure of $E(\bar{\mathbb{F}}_q)$ as an abelian group.

(3.4) PROPOSITION. *Let $\mathbb{F}_q$ be a finite field of characteristic p; let E be an elliptic curve over $\mathbb{F}_q$.*

(i) *The group $E(\bar{\mathbb{F}}_q)$ is a torsion group.*

(ii) *If $p \nmid n$ then $E(\bar{\mathbb{F}}_q)[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ as an abelian group.*

(iii) *If n is a power of p we have that*

$$E(\bar{\mathbb{F}}_q)[n] = \begin{cases} 0 & \text{if } E \text{ is supersingular;} \\ \mathbb{Z}/n\mathbb{Z} & \text{otherwise.} \end{cases}$$

Proof. (i) This is clear since $E(\bar{\mathbb{F}}_q) = \bigcup_k E(\mathbb{F}_{q^k})$.

(ii) and (iii) See [17].

(3.5) DEFINITION. *Let E be an elliptic curve over $\mathbb{F}_q$.* The *Frobenius endomorphism* $\phi \in \mathrm{End}_{\mathbb{F}_q}(E)$ is the endomorphism of E that acts on $E(\mathbb{F}_q)$ by raising the coordinates of the points to the qth power: in terms of Eq. (1) we have that $\phi(x:y:z) = (x^q:y^q:z^q)$.

Note that the kernel of $\phi - 1 \in \mathrm{End}_{\mathbb{F}_q}(E)$ acting on $E(\bar{\mathbb{F}}_q)$ is precisely $E(\mathbb{F}_q)$.

(3.6) PROPOSITION. *Let E be an elliptic curve over $\mathbb{F}_q$. Let ϕ denote its Frobenius endomorphism in* $\mathrm{End}_{\mathbb{F}_q}(E)$. *Let p denote the characteristic of $\mathbb{F}_q$.*

(i) *The endomorphism ϕ satisfies a unique equation $\phi^2 - t\phi + q = 0$ in* $\mathrm{End}_{\mathbb{F}_q}(E)$; *here $t \in \mathbb{Z} \subset \mathrm{End}_{\mathbb{F}_q}(E)$.*

(ii) $|t| \leqslant 2\sqrt{q}$.

(iii) $\#E(\mathbb{F}_q) = N(\phi - 1) = q + 1 - t$.

(iv) *$p \mid t$ if and only if E is supersingular.*

Proof. See [17].

The integer t is $T(\phi)$, the trace of the Frobenius endomorphism.

(3.7) PROPOSITION. *Let E be an elliptic curve over $\mathbb{F}_q$; let p be the characteristic of $\mathbb{F}_q$. Let $n \in \mathbb{Z}_{\geqslant 1}$ with $p \nmid n$ and let t denote the trace of the Frobenius endomorphism ϕ of E. The following are equivalent:*

(i) $E(\bar{\mathbb{F}}_q)[n] \subset E(\mathbb{F}_q)$.

(ii) $n^2 \mid q+1-t$, $n \mid q-1$ *and either* $\phi \in \mathbb{Z}$ *or*

$$\mathcal{O}\left(\frac{t^2-4q}{n^2}\right) \subset \mathrm{End}_{\mathbb{F}_q}(E).$$

Proof. The canonical map $\mathrm{End}_{\mathbb{F}_q}(E)/n\,\mathrm{End}_{\mathbb{F}_q}(E) \hookrightarrow \mathrm{End}(E(\bar{\mathbb{F}}_q)[n])$ is injective; see [16].

We see that (i) is equivalent to

$$\frac{\phi-1}{n} \in \mathrm{End}_{\mathbb{F}_q}(E).$$

If $\phi \in \mathbb{Z}$ this is clearly equivalent to

$$n^2 \mid q+1-t \quad \text{and} \quad n \mid q-1$$

since $q=\phi^2$ and $q+1-t=(\phi-1)^2$. If $\phi \notin \mathbb{Z}$ we compute

$$N\left(\frac{\phi-1}{n}\right)=\frac{q+1-t}{n},$$

$$T\left(\frac{\phi-1}{n}\right)=\frac{t-2}{n}=\frac{q-1}{n}-\frac{q+1-t}{n},$$

and

$$\Delta\left(\mathbb{Z}\left[\frac{\phi-1}{n}\right]\right)=T\left(\frac{\phi-1}{n}\right)^2-4N\left(\frac{\phi-1}{n}\right)=\frac{t^2-4q}{n^2}$$

so (i) is equivalent to

$$\frac{q+1-t}{n^2} \quad \text{and} \quad \frac{q-1}{n} \in \mathbb{Z} \quad \text{and} \quad \mathcal{O}\left(\frac{t^2-4q}{n^2}\right) \subset \mathrm{End}_{\mathbb{F}_q}(E),$$

which is precisely (ii). This proves the proposition.

4. Isogeny Classes of Elliptic Curves

Let $\mathbb{F}_q$ be a finite field of characteristic p.

(4.1) Definition. Two elliptic curves over $\mathbb{F}_q$ are called *isogenous* over $\mathbb{F}_q$ if they have the same number of points defined over $\mathbb{F}_q$. By $I(t)$ we denote the isogeny class of elliptic curves that have exactly $q+1-t$ points defined over $\mathbb{F}_q$. By $N(t)$ we denote the number of $\mathbb{F}_q$-isomorphism classes in $I(t)$.

Our definition agrees with the usual one; see [16].

(4.2) THEOREM. *For every integer $t \in \mathbb{Z}$, the number $N(t)$ is not zero if and only if one of the following holds*:

(i) $p \nmid t$ *and* $t^2 \leqslant 4q$;

(ii) *the degree* $[\mathbb{F}_q:\mathbb{F}_p]$ *is odd and one of the following holds*

(1) $t=0$;

(2) $t=\pm\sqrt{2q}$ *and* $p=2$;

(3) $t=\pm\sqrt{3q}$ *and* $p=3$;

(iii) *the degree* $[\mathbb{F}_q:\mathbb{F}_p]$ *is even and one of the following holds*

(1) $t=\pm 2\sqrt{q}$;

(2) $t=\pm\sqrt{q}$ *and* $p \not\equiv 1 \pmod 3$;

(3) $t=0$ *and* $p \not\equiv 1 \pmod 4$.

Proof. See Waterhouse's thesis [19, Theorem (4.1)].

The following theorem describes which rings occur as rings of $\mathbb{F}_q$-endomorpisms of elliptic curves defined over $\mathbb{F}_q$.

(4.3) THEOREM. *Let $t \in \mathbb{Z}$ be one of the numbers listed in Theorem* (4.2). *The set $I(t)$ is not empty and the following rings are precisely the ones that occur as rings of $\mathbb{F}_q$-endomorphisms of some elliptic curve in $I(t)$*:

(i) *if $p \nmid t$: all complex quadratic orders containing $\mathcal{O}(t^2-4q)$;*

(ii) *if $t=\pm 2\sqrt{q}$: all maximal orders in $\mathbb{Q}_{\infty,p}$;*

(iii) *if $p \mid t$ and $t \neq \pm 2\sqrt{q}$: all complex quadratic orders $\mathcal{O}$ with*

$$\mathcal{O}(t^2-4q) \subset \mathcal{O} \qquad \text{and} \qquad p \nmid [\mathcal{O}_{\max}:\mathcal{O}].$$

Proof. See Waterhouse's thesis [19, Theorem (4.2)].

The curves E in (i) and (ii) have all their endomorphisms defined over $\mathbb{F}_q$, that is $\mathrm{End}_{\mathbb{F}_q}(E)=\mathrm{End}_{\bar{\mathbb{F}}_q}(E)$.

For future reference we list the unit groups of the maximal orders in $\mathbb{Q}_{\infty,p}$. These groups are the groups of $\bar{\mathbb{F}}_q$-automorphisms of supersingular elliptic curves.

(4.4) PROPOSITION. (i) *Up to isomorphism there is exactly one maximal order in $\mathbb{Q}_{\infty,2}$; its group of units is isomorphic to $SL_2(\mathbb{F}_3)$. If E is a supersingular elliptic curve over $\bar{\mathbb{F}}_2$ then the action of* $\mathrm{Aut}_{\bar{\mathbb{F}}_2}(E)$ *on the* 3*-torsion points of E gives the isomorphism with $SL_2(\mathbb{F}_3)$.*

(ii) *Up to isomorphism there is exactly one maximal order in* $\mathbb{Q}_{\infty,3}$; *its group of units is isomorhic to a semidirect product of* $\mathbb{Z}/3\mathbb{Z}$ *by* $\mathbb{Z}/4\mathbb{Z}$, *the action of* $\mathbb{Z}/4\mathbb{Z}$ *on* $\mathbb{Z}/3\mathbb{Z}$ *being the non-trivial one.*

(iii) *If* $p \neq 2, 3$ *then the group of units of a maximal order in* $\mathbb{Q}_{\infty,p}$ *is either* μ_2, μ_4 *or* μ_6. *If* E *is a supersingular curve over* $\bar{\mathbb{F}}_p$ *then* $\mathrm{End}_{\bar{\mathbb{F}}_p}(E)$ *is a maximal order* $\mathcal{O}$ *in* $\mathbb{Q}_{\infty,p}$. *If the j-invariant of* E *equals* 0 *then* $\mathcal{O}^* = \mu_6$; *if the j-invariant of* E *equals* 1728 *then* $\mathcal{O}^* = \mu_4$. *In all other cases* $\mathcal{O}^* = \mu_2$.

Proof. See Tate [17, p. 182] or Deuring [8, Sect. 5].

Deuring gives in [8] normal forms for elliptic curves and an explicit description of the automorphisms. We will use Proposition (4.4) in Section 5.

Next we count the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves within a fixed $\mathbb{F}_q$-isogeny class with a given endomorphism ring.

(4.5) THEOREM. (i) *Let* $\mathcal{O}$ *be a complex quadratic order that occurs as the endomorphism ring of an elliptic curve over* $\mathbb{F}_q$ *in* $I(t)$. *Let* f *denote the residue class degree of* p *in* $\mathcal{O}$; *so* $f = 2$ *if* $(\Delta(\mathcal{O})/p) = -1$ *and* $f = 1$ *otherwise. The number of* $\mathbb{F}_q$*-isomorphism classes of curves* E *in* $I(t)$ *with* $\mathrm{End}_{\mathbb{F}_q}(E) = \mathcal{O}$ *equals* $f \cdot h(\mathcal{O})$.

(ii) *Let* $\mathcal{O}$ *be a maximal order in* $\mathbb{Q}_{\infty,p}$ *that occurs as the endomorphism ring of an elliptic curve over* $\mathbb{F}_q$ *in* $I(t)$. *The number of curves* E *in* $I(t)$ *with* $\mathrm{End}_{\mathbb{F}_q}(E) = \mathcal{O}$ *equals* 1 *or* 2. *It equals* 1 *if the prime over* p *in* $\mathcal{O}$ *is principal and* 2 *otherwise.*

Proof. This is Theorem (4.5) of Waterhouse [19]. There is a slight error in Theorem (4.5) as stated in [19]. The error is in the deduction of this theorem from the results of Chap. 5 of [19]. In fact, if $\mathcal{O}$ is commutative, the set of isomorphism classes of elliptic curves with endomorphism ring equal to $\mathcal{O}$ need not be a principal homogeneous space over the class group of $\mathcal{O}$. There may be more orbits and it follows in fact from Theorem (5.3) of [19] that there are two orbits exactly when $\mathcal{O}$ is commutative and p is inert in $\mathcal{O}$ over $\mathbb{Z}$. In all other cases there is one orbit. This proves Theorem (4.5).

(4.6) THEOREM. *Let* $t \in \mathbb{Z}$; *the number* $N(t)$ *assumes the values*

$$
\begin{aligned}
N(t) &= H(t^2 - 4q) && \text{if } t^2 < 4q \text{ and } p \nmid t;\\
&= H(-4p) && \text{if } t = 0\\
&= 1 && \text{if } t^2 = 2q \text{ and } p = 2 \quad \left.\begin{array}{l}\text{and if } q \text{ is}\\ \text{not a square;}\end{array}\right.\\
&= 1 && \text{if } t^2 = 3q \text{ and } p = 3
\end{aligned}
$$

$$
\left.\begin{aligned}
&= \frac{1}{12}\left(p+6-4\left(\frac{-3}{p}\right)-3\left(\frac{-4}{p}\right)\right) && \text{if } t^2=4q \\
&= 1-\left(\frac{-3}{p}\right) && \text{if } t^2=q \\
&= 1-\left(\frac{-4}{p}\right) && \text{if } t=0
\end{aligned}\right\} \text{and if } q \text{ is a square;}
$$

$$
= 0 \qquad \text{otherwise.}
$$

Proof. In view of Theorem (4.2) we already know the values of t for which $N(t)=0$. Let therefore E be an elliptic curve over $\mathbb{F}_q$ with $q+1-t$ points over $\mathbb{F}_q$. We will use Theorem (4.3) to figure out which rings occur as rings of endomorphisms of elliptic curves in $I(t)$ and then apply Theorem (4.5) to count the curves in $I(t)$ that have a given endomorphism ring.

First we consider the case where $p \nmid t$. According to Theorem (4.3)(i) all complex quadratic orders $\mathcal{O}$ containing $\mathcal{O}(t^2-4q)$ occur as the endomorphism ring of an elliptic curve in $I(t)$. Since the discriminants of $\mathcal{O}$ and $\mathcal{O}(t^2-4q)$ differ by a square and since $((t^2-4q)/p)=1$ we conclude from Theorem (4.5)(i) that exactly $h(\mathcal{O})$ elliptic curves in $I(t)$ have $\mathcal{O}$ as their ring of $\mathbb{F}_q$-endomorphisms. We find that

$$
N(t) = \sum_{\mathcal{O}(t^2-4q)\subset\mathcal{O}\subset\mathcal{O}_{\max}} h(\mathcal{O}) = H(t^2-4q)
$$

by Proposition (2.4).

Next we consider the cases where the curves in $I(t)$ are supersingular, that is, the cases where $p \mid t$. First we consider the case where $\mathrm{End}_{\mathbb{F}_q}(E)$ is commutative; from Theorem (4.2) and Theorem (4.3)(iii) it follows that $t^2=0$, q, $2q$, or $3q$ in this case. Since all computations look very much alike in these cases, we will do just one as an example: suppose $t=\sqrt{q}$; so q is a square and according to Theorem (4.2)(iii) we have that $N(t)=0$ if and only if $p\equiv 1 \pmod 3$. Suppose that $p \not\equiv 1 \pmod 3$. We have that $t^2-4q=-3q$; the maximal order containing $\mathcal{O}(-3q)$ is $\mathcal{O}(-3)$ and the only order $\mathcal{O}$ with $\mathcal{O}(-3q)\subset\mathcal{O}\subset\mathcal{O}(-3)$ that has $p \nmid [\mathcal{O}(-3):\mathcal{O}]$ is $\mathcal{O}(-3)$ itself. By Theorem (4.3)(iii) we must have that the ring of $\mathbb{F}_q$-endomorphisms of E equals $\mathcal{O}(-3)=\mathbb{Z}[\zeta]$. The class number $h(-3)$ equals 1 and in the notation of Theorem (4.5)(i) we have that $f=2$ if $(-3/p)=-1$ and $f=1$ if $(-3/p)=0$. Since $I(t)=\varnothing$ if $p\equiv 1 \pmod 3$ we conclude from Theorem (4.5)(i) that

$$
N(t) = \#I(t) = 1-\left(\frac{-3}{p}\right).
$$

The other cases where $t \neq \pm 2\sqrt{q}$ can be checked in an analogous way.

Finally we consider the cases where $t = \pm 2\sqrt{q}$. In these cases the curves in $I(t)$ have a noncommutative endomorphism ring viz. a maximal order in $\mathbb{Q}_{\infty,p}$. By Theorem (4.5)(ii) the total number of curves in $I(t)$ equals the number of maximal orders in $\mathbb{Q}_{\infty,p}$ in which the prime over p is principal plus twice the number of the other maximal orders. This is precisely the class number of $\mathbb{Q}_{\infty,p}$; its value is $\frac{1}{12}(p+6-4(-3/p)-3(-4/p))$, see [8, pp. 199–200]. This proves Theorem (4.6).

We have now counted the number of isomorphism classes of elliptic curves over $\mathbb{F}_q$ with a given number of points defined over $\mathbb{F}_q$. In the rest of this section we will count elliptic curves in $I(t)$ which have some special properties. We will need these results in Section 5.

(4.7) DEFINITION. For every $n \in \mathbb{Z}_{\geqslant 1}$, let

$$N_n(t) = \#\{\mathbb{F}_q\text{-isomorphism classes of elliptic curves } E \text{ in } I(t) \text{ with } n \mid \#E(\mathbb{F}_q)\},$$

$$N_{n\times n}(t) = \#\{\mathbb{F}_q\text{-isomorphism classes of elliptic curves } E \text{ in } I(t) \text{ with } E(\mathbb{F}_q)[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}\}.$$

We clearly have that

$$N_n(t) = N(t) \quad \text{if} \quad t \equiv q+1 \pmod{n},$$
$$= 0 \quad \text{otherwise;}$$

because all curves E in $I(t)$ have $\#E(\mathbb{F}_q) = q+1-t$.

In the rest of this section we will compute the values of $N_{n\times n}(t)$: the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves in $I(t)$ which have exactly n^2 points in $E(\mathbb{F}_q)[n]$.

(4.8) LEMMA. *Let $t \in \mathbb{Z}$.*

(i) *If $t^2 = q$, $2q$, or $3q$ then every curve E in $I(t)$ has $E(\mathbb{F}_q)$ cyclic.*

(ii) *If $t^2 = 4q$ then every curve E in $I(t)$ has $E(\mathbb{F}_q) \cong \mathbb{Z}/(\sqrt{q}\pm 1)\,\mathbb{Z} \oplus \mathbb{Z}/(\sqrt{q}\pm 1)\,\mathbb{Z}$; we have the minus signs if $t = 2\sqrt{q}$ and the plus signs if $t = -2\sqrt{q}$.*

(iii) *If $q \not\equiv -1 \pmod 4$ every curve E in $I(0)$ has $E(\mathbb{F}_q)$ cyclic. If $q \equiv -1 \pmod 4$ then exactly $h(-4p)$ curves in $I(0)$ have $E(\mathbb{F}_q)$ cyclic; the other $h(-p)$ curves have $E(\mathbb{F}_q) \cong \mathbb{Z}/((q+1)/2)\,\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.*

Proof. Suppose $t^2 = \alpha q$ with $\alpha = 0$, 1, 2, or 3; let E be an elliptic curve over $\mathbb{F}_q$ in $I(t)$ which has $E(\mathbb{F}_q)[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$; this implies that $p \nmid n$ by

Proposition (3.4)(iii). From Proposition (3.7) we see that $n^2 | q+1-t$ and $n | q-1$; this implies that $n | 4-\alpha$. If $\alpha = 3$ this implies that $n = 1$. If $\alpha = 2$ we must have that $p = 2$ and the fact that $p \nmid n$ implies that $n = 1$. If $\alpha = 1$ and $n = 3$ we see that $9 | q+1 \pm \sqrt{q}$ which is impossible; we conclude that $n = 1$. If $\alpha = 0$ we have that $n | 4$; if $q \not\equiv -1 \pmod 4$ we conclude from $n^2 | q+1-t$ that $n = 1$; if $q \equiv -1 \pmod 4$ we see from $n | q-1$ that $n = 1$ or 2.

Suppose that $q \equiv -1 \pmod 4$ and let E be an elliptic curve in $I(0)$. From the fact that q is not a square and Theorem (4.3) we conclude that the possible endomorphism rings for E are $\mathcal{O}(-4p)$ and $\mathcal{O}(-p)$. Since $\mathcal{O}(-q) \subset \mathcal{O}(-p)$ and $\mathcal{O}(-q) \not\subset \mathcal{O}(-4p)$ we conclude from Proposition (3.7) that $E(\bar{\mathbb{F}}_q)[2] \subset E(\mathbb{F}_q)$ if and only if $\mathrm{End}_{\mathbb{F}_q}(E) = \mathcal{O}(-p)$. Since p ramifies in both $\mathcal{O}(-p)$ and $\mathcal{O}(-4p)$, Theorem (4.5)(i) implies that exactly $h(-p)$ curves have $\mathcal{O}(-p)$ as their endomorphism ring; by the above discussion these curves E have $E(\mathbb{F}_q) \cong \mathbb{Z}/((q+1)/2)\,\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. The other $h(-4p)$ curves in $I(0)$ have $E(\mathbb{F}_q)$ cyclic.

Finally suppose that $t = 2\sqrt{q}$ and that E is an elliptic curve in $I(t)$. The Frobenius endomorphism ϕ of E equals $\sqrt{q} \in \mathbb{Z}$. We have that $\#E(\mathbb{F}_q) = q+1-t = (\sqrt{q}-1)^2$. Proposition (3.7) implies that $E(\bar{\mathbb{F}}_q)\,[\sqrt{q}-1] \subset E(\mathbb{F}_q)$; since both sets have the same cardinality we have that

$$E(\mathbb{F}_q) = E(\bar{\mathbb{F}}_q)[\sqrt{q}-1] \cong \mathbb{Z}/(\sqrt{q}-1)\,\mathbb{Z} \oplus \mathbb{Z}/(\sqrt{q}-1)\,\mathbb{Z}.$$

The proof for $t = -2\sqrt{q}$ is analogous. This proves Lemma (4.8).

(4.9) THEOREM. *Suppose that $n \in \mathbb{Z}_{\geqslant 1}$ is odd and that $t \in \mathbb{Z}$ satisfies $t^2 \leqslant 4q$.*

(i) *If $p \nmid t$, $q \equiv 1 \pmod n$ and $t \equiv q+1 \pmod{n^2}$ then*

$$N_{n\times n}(t) = H\left(\frac{t^2-4q}{n^2}\right);$$

(ii) *if $\sqrt{q} \equiv 1 \pmod n$ then $N_{n\times n}(2\sqrt{q}) = N(2\sqrt{q})$;*

(iii) *if $\sqrt{q} \equiv -1 \pmod n$ then $N_{n\times n}(-2\sqrt{q}) = N(-2\sqrt{q})$.*

In all other cases $N_{n\times n}(t) = 0$.

Proof. Suppose that $P \nmid t$. According to Proposition (3.7) the number $N_{n\times n}(t)$ equals 0 whenever $n^2 \nmid q+1-t$ or $n \nmid q-1$. Let us assume that $n^2 | q+1-t$ and that $n | q-1$. By Proposition (3.7) a curve E in $I(t)$ has $E(\mathbb{F}_q)[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ if and only if

$$\mathcal{O}\left(\frac{t^2-4q}{n^2}\right) \subset \mathrm{End}_{\mathbb{F}_q}(E);$$

this implies that

$$N_{n\times n}(t)=\sum_{\mathcal{O}((t^2-4q)/n^2)\subset\mathcal{O}\subset\mathcal{O}_{\max}} h(\mathcal{O})=H\left(\frac{t^2-4q}{n^2}\right)$$

by Proposition (2.4). This proves (ii).

Next suppose that $p\mid t$. From Theorem (4.2), Lemma (4.8) and the fact that n is odd we see that $N_{n\times n}(t)$ is not zero except when $t=2\sqrt{q}\equiv 2 \pmod n$ or $t=-2\sqrt{q}\equiv -2 \pmod n$. In these cases all curves in $I(t)$ have that $E(\mathbb{F}_q)[n]\cong\mathbb{Z}/n\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}$. This proves the theorem.

5. Nonsingular Plane Cubics over Finite Fields

In this section we will compute the number of equivalence classes of nonsingular plane cubic curves over a finite field $\mathbb{F}_q$ with a given number of points defined over $\mathbb{F}_q$. The main result is given in Theorem (5.2).

(5.1) Lemma. *Let q be a power of a prime p.*

(i) *If $p\equiv 1 \pmod 3$ there is exactly one solution*

$$t\in\mathbb{Z} \text{ to } \begin{cases} t\equiv q+1 \pmod 9 \\ t^2+3x^2=4q \quad \text{for some } x\in\mathbb{Z} \\ p\nmid t. \end{cases}$$

(ii) *If $p\equiv 1 \pmod 4$ and $q\equiv 1 \pmod 3$ there is exactly one solution*

$$t\in\mathbb{Z} \text{ to } \begin{cases} t\equiv q+1 \pmod 9 \\ t^2+4x^2=4q \quad \text{for some } x\in\mathbb{Z} \\ p\nmid t. \end{cases}$$

Proof. The proof of this lemma is an exercise in elementary number theory and is left to the reader.

If $q\equiv 1 \pmod 3$ we define $t_0\in\mathbb{Z}$ as follows:

$$t_0=\text{the unique solution in Lemma (5.1)(i)} \quad \text{if } p\equiv 1 \pmod 3$$
$$=2\left(\frac{\sqrt{q}}{3}\right)\sqrt{q} \quad \text{if } p\not\equiv 1 \pmod 3.$$

If $q\equiv 1$ or $4 \pmod{12}$ we define $t_1\in\mathbb{Z}$ as follows:

$$t_1=\text{the unique solution in Lemma (5.1)(ii)} \quad \text{if } p\equiv 1 \pmod 4$$
$$=2\left(\frac{\sqrt{q}}{3}\right)\sqrt{q} \quad \text{if } p\not\equiv 1 \pmod 4.$$

(5.2) THEOREM. *Let $\mathbb{F}_q$ be a finite field of characteristic p; let $M(t)$ denote the number of projectively inequivalent nonsingular plane cubic curves that have exactly $q+1-t$ points defined over $\mathbb{F}_q$. We have*

$$M(t) = N(t) + N_3(t) + 3N_{3\times 3}(t) - \varepsilon(t),$$

where

$$\begin{aligned} \varepsilon(t) &= 2 \quad \text{if} \quad (t = t_0 \text{ or } t = t_1) \text{ and } t_0 \neq t_1, \\ &= 3 \quad \text{if} \quad t = t_0 = t_1 \text{ and } p = 2, \\ &= 4 \quad \text{if} \quad t = t_0 = t_1 \text{ and } p \neq 2, \\ &= 0 \quad \text{otherwise.} \end{aligned}$$

We will give a proof of Theorem (5.2) after Lemma (5.6).

Remark. The definitions of t_0 and t_1 are given above; the values of $N(t)$, $N_3(t)$ and $N_{3\times 3}(t)$ are given in Theorem (4.6), Definition (4.7), and Theorem (4.9). These values are easily computable, their computation involves the calculation of certain class numbers, a table of which is given in Section 6.

(5.3) EXAMPLE. Nonsingular plane cubics over $\mathbb{F}_4$. It follows from Theorem (4.6) and Theorem (5.2) that $M(t)$ and $N(t)$ equal zero whenever $|t| > 4$.

t	$q+1-t$	t^2-4q	$N(t)$	$N_3(t)$	$N_{3\times 3}(t)$	$\varepsilon(t)$	$M(t)$
4	1		1	0	0	0	1
3	2	−7	1	0	0	0	1
2	3		2	2	0	0	4
1	4	−15	2	0	0	0	2
0	5		1	0	0	0	1
−1	6	−15	2	2	0	0	4
−2	7		2	0	0	0	2
−3	8	−7	1	0	0	0	1
−4	9		1	1	1	3	2

To obtain the entries of this table: use Theorem (4.6) to obtain the values of $N(t)$; a table of class numbers is given in Section 6; we have that $H(-7) = 1$ and $H(-15) = 2$. The value of $N_3(t)$ follows easily from Definition (4.7). Theorem (4.9) gives the values of $N_{3\times 3}(t)$ and we get the values of $\varepsilon(t)$ from the fact that $t_0 = t_1 = -4$ in this case.

The table is in agreement with the one given in [6].

Before we give a proof of Theorem (5.2) we translate the notion of projective equivalence of nonsingular plane cubic curves into something concerning elliptic curves.

A projective equivalence class of nonsingular plane cubic curves is the same as an equivalence class of closed immersions $i: E \subsetneq \mathbb{P}^2$, defined over $\mathbb{F}_q$, where E is an elliptic curve and $i(E)$ is of degree 3. Here we call two closed immersions $i_1: E_i \to \mathbb{P}^2$ and $i_2: E_2 \to \mathbb{P}^2$ equivalent if there is a commutative diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{i_1} & \mathbb{P}^2 \\ \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_2} \\ E_2 & \xrightarrow{i_2} & \mathbb{P}^2 \end{array}$$

with ϕ_1 and ϕ_2 isomorphisms of schemes.

The one-to-one correspondence between these equivalence classes follows from the fact that every nonsingular plane cubic curve over $\mathbb{F}_q$ has a point defined over $\mathbb{F}_q$ by [17] and the fact that the group of automorphisms of $\mathbb{P}^2$ over $\mathbb{F}_q$ as a scheme is precisely $PGL_2(\mathbb{F}_q)$, see [11, II.7.1.1].

Note that if $i: E \subsetneq \mathbb{P}^2$ is a closed immersion defined over $\mathbb{F}_q$ of an elliptic curve E, there is a one-to-one correspondence between $E(\mathbb{F}_q)$ and the $\mathbb{F}_q$-rational points of $i(E)$. Instead of counting nonsingular plane cubics up to projective equivalence with a given number of points defined over $\mathbb{F}_q$, we will count elliptic curves E over $\mathbb{F}_q$ furnished with a closed immersion $i: E \subsetneq \mathbb{P}^2$ of degree 3 according to $\#E(\mathbb{F}_q)$ upto our notion of equivalence.

Let E be an elliptic curve over $\mathbb{F}_q$ and let $i: E \subsetneq \mathbb{P}^2$ be a closed immersion over $\mathbb{F}_q$ of degree 3. The sheaf $i^*\mathcal{O}(1)$ is a very ample invertible sheaf $\mathcal{L}(D)$; we have that D is a divisor of degree 3 see Hartshorne [11, II.6.1.3, IV.3.3.2, and IV.3.3.3]. All sheaves and divisors are defined over $\mathbb{F}_q$: the only fact one uses to associate a divisor of degree 3 to the immersion i is the theorem of Riemann–Roch which is valid over any base field.

(5.4) PROPOSITION. *Let $\mathbb{F}_q$ be a finite field. There is a one-to-one correspondence between the following two sets*

projective equivalence classes of nonsingular plane cubic curves X defined over $\mathbb{F}_q$

and

isomorphism classes of pairs (E, P), where E is an elliptic curve defined over $\mathbb{F}_q$ and P an $\mathrm{Aut}_{\mathbb{F}_q}(E)$-orbit of $E(\mathbb{F}_q)$ [3].

Moreover, if a plane cubic curve X corresponds to a pair (E, P), the number of $\mathbb{F}_q$-rational points of X equals $\#E(\mathbb{F}_q)$.

Here, we call two pairs (E_1, P_1) and (E_2, P_2) isomorphic if there is an isomorphism $f: E_1 \xrightarrow{\sim} E_2$ of elliptic curves (Definition (3.2)) mapping the orbit P_1 to P_2.

Proof. By the above discussion we have a one-to-one correspondence between "equivalence classes of plane nonsingular cubic curves" and "closed immersions of degree 3 of elliptic curves in $\mathbb{P}^2$ upto a certain equivalence." A plane cubic corresponding to an immersion $i: E \subsetneq \mathbb{P}^2$ has as many points defined over $\mathbb{F}_q$ as E. To any closed immersion $i: E \subsetneq \mathbb{P}^2$ of degree 3 over $\mathbb{F}_q$ we can associate a divisor D of degree 3; this divisor is defined over $\mathbb{F}_q$ and only its class is determined by i, see [11, II.6.1.3]. It follows from [11, II.7.1(b)] that the divisor classes of degree 3 of E that are defined over $\mathbb{F}_q$ or the $\mathbb{F}_q$-divisor classes of degree 3 for short, up to action of the group of automorphisms of E as a scheme over $\mathbb{F}_q$, are in one-to-one correspondence with the equivalence classes of closed immersions $i: E \subsetneq \mathbb{P}^2$ as defined above.

The group of automorphisms of E as a scheme over $\mathbb{F}_q$ is generated by the group of translations by points in $E(\mathbb{F}_q)$ and by the group $\mathrm{Aut}_{\mathbb{F}_q}(E)$, the automorphisms of E as an elliptic curve (Definition (3.2)). The $\mathbb{F}_q$-divisor classes of degree 3 of E up to translations by $E(\mathbb{F}_q)$ are in one-to-one correspondence with $E(\mathbb{F}_q)/3E(\mathbb{F}_q)$ via $D \mapsto D - 3(0)$. Here 0 denotes the zero-element of E and we identify $E(\mathbb{F}_q)$ with the group of $\mathbb{F}_q$-divisor classes of degree 0 via $P \mapsto (P) - (0)$.

From the above we conclude that projective equivalence classes of plane cubic curves correspond one-to-one with pairs (E, x) where E is an elliptic curve and $x \in E(\mathbb{F}_q)/3E(\mathbb{F}_q)$, up to action of $\mathrm{Aut}_{\mathbb{F}_q}(E)$.

We have that $E(\mathbb{F}_q)[3]$ and $E(\mathbb{F}_q)/3E(\mathbb{F}_q)$ are isomorphic $\mathrm{Aut}_{\mathbb{F}_q}(E)$-modules. This is obvious if $\#E(\mathbb{F}_q)[3]$ is 1 or 3; if $\#E(\mathbb{F}_q)[3] = 9$ consider the $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$-cohomology sequence of the exact sequence

$$0 \to E(\mathbb{F}_q)[3] \to E(\bar{\mathbb{F}}_q) \xrightarrow{3} E(\bar{\mathbb{F}}_q) \to 0;$$

we get

$$E(\mathbb{F}_q)/3E(\mathbb{F}_q) \cong H^1(\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q), E(\mathbb{F}_q)[3])$$
$$\cong \mathrm{Hom}(\hat{\mathbb{Z}}, E(\mathbb{F}_q)[3]) \cong E(\mathbb{F}_q)[3]$$

as $\mathrm{Aut}_{\mathbb{F}_q}(E)$-modules.

It follows that the pairs (E, x) from above correspond one-to-one with pairs (E, P) where P is an $\mathrm{Aut}_{\mathbb{F}_q}(E)$-orbit of $E(\mathbb{F}_q)[3]$. This proves Proposition (5.4).

In the proof of Theorem (5.2) we need to know the number of $\mathrm{Aut}_{\mathbb{F}_q}(E)$-orbits of $E(\mathbb{F}_q)[3]$.

(5.5) PROPOSITION. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of*

characteristic p; let j denote the j-invariant of E. The number of $\mathrm{Aut}_{\mathbb{F}_q}(E)$*-orbits of* $E(\mathbb{F}_q)$ [3] *equals*

$$
\begin{array}{ll}
1 & \text{if } \#E(\mathbb{F}_q)[3]=1 \\
2 & \text{if } \#E(\mathbb{F}_q)[3]=3 \\
2 & \text{if } \#E(\mathbb{F}_q)[3]=9,\ p=2 \text{ and } j=0=1728 \\
3 & \text{if } \#E(\mathbb{F}_q)[3]=9,\ p\neq 2 \text{ and } j\in\{0,1728\} \\
5 & \text{if } \#E(\mathbb{F}_q)[3]=9 \text{ and } j\notin\{0,1728\}
\end{array}
$$

Proof. Note that always $-1\in\mathrm{Aut}_{\mathbb{F}_q}(E)$ and that $\mathrm{Aut}_{\mathbb{F}_q}(E)=\{\pm 1\}$ whenever $j\neq 0$ or 1728; this follows from Proposition (4.4). Suppose that $p=2$, that the j-invariant of E is 0 and that $\#E(\mathbb{F}_q)[3]=9$; then by Proposition (3.7) we must have that $\mathbb{F}_4\subset\mathbb{F}_q$; since E is supersingular we have by Lemma (4.8) that $E\in I(\pm 2\sqrt{q})$ and by the remark after Theorem (4.3) that E has all its automorphisms defined over $\mathbb{F}_q$. By Proposition (4.4)(i) we have that $\mathrm{Aut}_{\mathbb{F}_q}(E)=SL_2(\mathbb{F}_3)$; this group acts transitively on $E(\mathbb{F}_q)[3]-\{0\}$ so $\mathrm{Aut}_{\mathbb{F}_q}(E)$ has two orbits in $E(\mathbb{F}_q)$.

If $p\neq 2$, $j\in\{0,1728\}$ and $E(\mathbb{F}_q)[3]=9$ then either j is supersingular and by Lemma (4.8) the curve E is in $I(\pm 2\sqrt{q})$, or j is not supersingular; in both cases all endomorphisms are defined over $\mathbb{F}_q$ and it follows from Proposition (4.4)(iii) and the remarks after Definition (3.3) that $\mathrm{Aut}_{\mathbb{F}_q}(E)=\mu_6$ if $j=0$ and that $\mathrm{Aut}_{\mathbb{F}_q}(E)=\mu_4$ if $j=1728$. In both cases there are three $\mathrm{Aut}_{\mathbb{F}_q}(E)$-orbits in $E(\mathbb{F}_q)$ [3].

All other statements are clear.

(5.6) LEMMA. *Let* $\mathbb{F}_q$ *be a finite field.*

(i) *There is at most one elliptic curve E with* $j=0$ *and* $\#E(\mathbb{F}_q)[3]=9$. *There is exactly one if and only if* $q\equiv 1 \pmod 3$ *and this curve has the trace of its Frobenius endomorphism equal to* t_0.

(ii) *There is at most one elliptic curve E with* $j=1728$ *and* $\#E(\mathbb{F}_q)[3]=9$. *There is exactly one if and only if* $q\equiv 1$ *or* $4 \pmod{12}$ *and this curve has the trace of its Frobenius endomorphism equal to* t_1.

Proof. (i) If there is an elliptic curve E over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q)[3]=9$ it follows from Proposition (3.7) that $q\equiv 1 \pmod 3$. Suppose, on the other hand, that $q\equiv 1 \pmod 3$. If $p\not\equiv 1 \pmod 3$ then every curve E with j-invariant equal to 0 is supersingular. Lemma (4.8) implies that a curve E with $j=0$ and $\#E(\mathbb{F}_q)[3]=9$ must be in $I(2(\sqrt{q}/3)\sqrt{q})$ and there is, in fact, exactly one in $I(2(\sqrt{q}/3)\sqrt{q})$. If $p\equiv 1 \pmod 3$, let E denote a curve with j-invariant equal to 0. We have $\mathrm{End}_{\mathbb{F}_q}(E)=\mathcal{O}(-3)=\mathbb{Z}[\zeta]$. Let t denote the trace of the Frobenius endomorphism of E. We have that $p\nmid t$

and that $t^2+3x^2=4q$ for some $x\in\mathbb{Z}$. Proposition (3.7) implies that $\#E(\mathbb{F}_q)[3]=9$ if and only if $t\equiv q+1 \pmod 9$. The result now follows from Lemma (5.1) and the fact that the class number of $\mathcal{O}(-3)$ is one.

(ii) If there is an elliptic curve E over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q)[3]=9$ and j-invariant equal to 1728, it follows from Proposition (3.7) that $q\equiv 1 \pmod 3$. If $p\not\equiv 1 \pmod 4$ the curve E is supersingular and by Lemma (4.8) we must have that $E\in I(\pm 2\sqrt{q})$ and that q is a square. Since $p\neq 3$ this implies that $q\equiv 1$ or $4 \pmod{12}$. The rest of the proof is analogous to the proof of (i).

This proves the lemma.

Proof of Theorem (5.2). It follows from Proposition (5.4) that $M(t)$ equals the number of isomorphism classes of pairs (E, P) where E is an elliptic curve with $\#E(\mathbb{F}_q)=q+1-t$ and P is an $\mathrm{Aut}_{\mathbb{F}_q}(E)$-orbit of $E(\mathbb{F}_q)[3]$. If E does not have nine 3-torsion points over $\mathbb{F}_q$ or if the j-invariant of E is not in $\{0, 1728\}$ it follows from Proposition (5.5) that we have 1, 2, or 5 of pairs (E, P) according as $\#E(\mathbb{F}_q)=1, 3$, or 9. So, if there is no curve in $I(t)$ with $j\in\{0, 1728\}$ and $\#E(\mathbb{F}_q)[3]=9$, we have that

$$\begin{aligned} M(t) &= \#\{\text{curves } E \text{ in } I(t) \text{ with } \#E(\mathbb{F}_q)[3]=1\} \\ &\quad + 2\#\{\text{curves } E \text{ in } I(t) \text{ with } \#E(\mathbb{F}_q)[3]=3\} \\ &\quad + 5\#\{\text{curves } E \text{ in } I(t) \text{ with } \#E(\mathbb{F}_q)[3]=9\} \\ &= (N(t)-N_3(t))+2(N_3(t)-N_{3\times 3}(t))+5N_{3\times 3}(t) \\ &= N(t)+N_3(t)+3N_{3\times 3}(t). \end{aligned}$$

From Lemma (5.6) we see that this formula for $M(t)$ holds whenever $t\notin\{t_0, t_1\}$. If $t=t_0$ or t_1 there are curves in $I(t)$ with $j\in\{0, 1728\}$ and 9 rational 3-torsion points and there are less than five orbits. It follows from Proposition (5.5), Lemma (5.6), and the definition of ε that $M(t)=N(t)+N_3(t)+3N_{3\times 3}(t)-\varepsilon(t)$ for every $t\in\mathbb{Z}$. This proves Theorem (5.2).

Remark. From the proof of Theorem (5.2) we see at once that $M(t)\neq 0$ if and only if $N(t)\neq 0$ and we conclude that Theorem (4.2) is also valid with $N(t)$ replaced by $M(t)$.

We finish this section by calculating the total number of projectively inequivalent nonsingular plane cubic curves over a finite field $\mathbb{F}_q$. By Proposition (5.4) this number equals

$$\#\left\{\begin{array}{l}\text{isomorphic classes of pairs } (E, P), \text{ where } E \text{ is an elliptic} \\ \text{curve over } \mathbb{F}_q \text{ and } P \text{ an } \mathrm{Aut}_{\mathbb{F}_q}(E)\text{-orbit of } E(\mathbb{F}_q)[3]\end{array}\right\},$$

which equals

$$\#\{\text{isomorphism classes of elliptic curves } E \text{ over } \mathbb{F}_q\}$$
$$+\ \#\left\{\begin{array}{l}\text{isomorphism classes of pairs } (E, P), \text{ where } E \text{ is an elliptic}\\ \text{curve over } \mathbb{F}_q \text{ and } P \text{ a non-zero } \mathrm{Aut}_{\bar{\mathbb{F}}_q}(E)\text{-orbit of } E(\bar{\mathbb{F}}_q)\ [3]\end{array}\right\}$$

We compute the cardinality of these sets by counting the $\mathbb{F}_q$-rational points on the moduli spaces $X(1)$ and $X_1(3)$; see [7].

The curve $X(1)$ is simply the projective line: the j-line with a "cusp" which we call ∞.

(5.7) PROPOSITION. *Let $\mathbb{F}_q$ be a finite field. The number of isomorphism classes of elliptic curves over $\mathbb{F}_q$ equals*

$$2q+3+2\left(\frac{-3}{q}\right)+\left(\frac{-4}{q}\right).$$

(*Here $p=\mathrm{char}(\mathbb{F}_q)$, $q=p^k$ and $(x/q)=(x/p)^k$.*)

Proof. Let $j\in\mathbb{F}_q$; there exists a curve E over $\mathbb{F}_q$ with j-invariant equal to j; see [7, VI.1.6]. The number of curves over $\mathbb{F}_q$ that have their j-invariant equal to j equals $\#H^1(\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q), \mathrm{Aut}_{\bar{\mathbb{F}}_q}(E))$; see [7, VI.3.1]. Here the cohomology is in the sense of [14, p. 131]. If j is not 0 or 1728 we have that $H^1(\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q), \mathrm{Aut}_{\bar{\mathbb{F}}_q}(E))\cong \mathrm{Hom}(\hat{\mathbb{Z}}, \{\pm 1\})=\mathbb{Z}/2\mathbb{Z}$; if $j=0$ and $p\notin\{2,3\}$ we get from Proposition (4.4)(iii) and the remarks after Definition (3.3) that $\mathrm{Aut}_{\bar{\mathbb{F}}_q}(E)=\mu_6$ and if $j=1728$ and $p\notin\{2,3\}$ we get that $\mathrm{Aut}_{\bar{\mathbb{F}}_q}(E)=\mu_4$. A standard computation shows that if $p\notin\{2,3\}$ we have that

$$\#H^1(\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q), \mathrm{Aut}_{\bar{\mathbb{F}}_q}(E))=3+\left(\frac{-4}{q}\right) \qquad \text{if } j=1728$$
$$=4+2\left(\frac{-3}{q}\right) \qquad \text{if } j=0. \tag{1}$$

If $p=2$ or 3 one can use the fact that the curves with j-invariant equal to $0=1728$ are precisely the supersingular curves, that is, the curves that have the trace of the Frobenius endomorphism divisible by p. Theorem (4.6) gives a formula for the number of supersingular curves over $\mathbb{F}_q$. Alternatively one can use Lemma (4.4)(i) and (ii) and an explicit description of the action of $\mathrm{Aut}_{\bar{\mathbb{F}}_q}(E)$ as given in [8]. For example, suppose $p=2$ and $\mathbb{F}_4\subset\mathbb{F}_q$: in this case all endomorphisms of E are defined over $\mathbb{F}_q$ and the group $\mathrm{Aut}_{\bar{\mathbb{F}}_q}(E)$ is $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$-invariant; the pointed set $H^1(\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q), \mathrm{Aut}_{\bar{\mathbb{F}}_q}(E))$ is canonically isomorphic to the set of conjugacy classes of $\mathrm{Aut}_{\bar{\mathbb{F}}_q}(E)\cong SL_2(\mathbb{F}_3)$. There are seven conjugacy classes in $SL_2(\mathbb{F}_3)$.

The result is the following: if $p \in \{2, 3\}$ and the j-invariant of E equals $0 = 1728$ then

$$\#H^1(\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q), \mathrm{Aut}_{\bar{\mathbb{F}}_q}(E)) = 5 + 2\left(\frac{-3}{q}\right) + \left(\frac{-4}{q}\right). \tag{2}$$

The number of isomorphism classes of elliptic curves over $\mathbb{F}_q$ equals

$$\sum_{\infty \neq j \in X(1)(\mathbb{F}_q)} \#H^1(\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q), \mathrm{Aut}_{\bar{\mathbb{F}}_q}(E_j));$$

here E_j denotes an elliptic curve over $\mathbb{F}_q$ with j-invariant equal to j. By the above this sum equals

$$\sum_{j \in \{0,1728\}} \#H^1(\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q), \mathrm{Aut}_{\bar{\mathbb{F}}_q}(E)) + \begin{cases} 2(q-2) & \text{if } p \notin \{2, 3\} \\ 2(q-1) & \text{if } p \in \{2, 3\}. \end{cases}$$

The result now follows from formulas (1) and (2).

(5.8) PROPOSITION. *Let $\mathbb{F}_q$ be a finite field; the number of isomorphism classes of pairs (E, P), where E is an elliptic curve over $\mathbb{F}_q$ and $P \in E(\mathbb{F}_q)$ a point of order 3 equals*

$$\begin{cases} q-1 & \text{if } q \not\equiv 1 \pmod 3, \\ q+1 & \text{if } q \equiv 1 \pmod 3. \end{cases}$$

(Here two pairs (E_1, P_1) and (E_2, P_2) are called isomorphic if there is an isomorphism of elliptic curves $E_1 \to E_2$ mapping P_1 to P_2.)

Proof. Let p denote the characteristic of $\mathbb{F}_q$. We first consider the case where $p = 3$. In this case the supersingular curves E do not have points of order 3 in $E(\mathbb{F}_q)$. If $3 \nmid t$ it holds that the curves E in $I(t)$ have a point of order 3 if and only if the curves in $I(-t)$ do not. Since $\#E(\mathbb{F}_q)[3] \leqslant 3$ by Proposition (3.4)(iii) and since (E, P) is isomorphic to $(E, -P)$ for every elliptic curve E and every $P \in E(\mathbb{F}_q)[3]$ of order 3 we conclude that the number of isomorphism classes (E, P) over $\mathbb{F}_q$ equals half the number of non-supersingular curves, so it equals $q-1$ by Proposition (5.7) and formula (2).

Next we consider the case where $p \neq 3$. In this case the modular curve $X_1(3)$ is a nonsingular projective curve defined over $\mathbb{F}_q$ which admits a canonical morphism of degree 4 to $X(1)$ which is also defined over $\mathbb{F}_q$. This morphism is ramified over $j = 0, 1728$, and ∞; there are two points over $j = \infty$, the so-called cusps; one has ramification index 1 and the other has ramification index 3; both points are clearly defined over $\mathbb{F}_q$. If $p \neq 2$ exactly the same thing happens over $j = 0$: the point with ramification index

3 corresponds to the pair (E, P), where E is an elliptic curve over $\mathbb{F}_q$ with j-invariant equal to 0 and hence $\mathbb{Z}[\zeta] \subset \mathrm{End}_{\bar{\mathbb{F}}_q}(E)$ and where P is a point of order 3 annihilated by $\zeta - 1$. If $p \neq 2$, there are two points over $j = 1728$ each with ramification index equal to 2. If $p = 2$ we have that $0 = 1728$; in this case there is only one point in $X_1(3)$ over $j = 0$; it has ramification index 4. The Hurwitz formula for the genus shows that the genus of $X_1(3)$ is equal to 0. Since $X_1(3)$ has points over $\mathbb{F}_q$, it is isomorphic to $\mathbb{P}^1$ over $\mathbb{F}_q$. For all this see [15].

To every point $x \in X_1(3)(\mathbb{F}_q)$ which is not a cusp, there is a pair (E, P) defined over $\mathbb{F}_q$ see [7, VI.3.2]. The number of non-isomorphic pairs corresponding to x equals

$$\# H^1(\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q), \mathrm{Aut}_{\bar{\mathbb{F}}_q}((E, P)));$$

here $\mathrm{Aut}_{\bar{\mathbb{F}}_q}((E, P))$ denotes the group of $\bar{\mathbb{F}}_q$-automorphisms of E that leave P fixed. If $j \notin \{0, 1728\}$ we have for every curve E with j-invariant equal to j and $P \in E(\mathbb{F}_q)$ a point of order 3 that $\mathrm{Aut}_{\bar{\mathbb{F}}_q}(E) = \{\pm 1\}$ and $\mathrm{Aut}_{\bar{\mathbb{F}}_q}((E, P)) = \{1\}$. If $j = 1728$ and $p \notin \{2, 3\}$ we have that $\mathrm{Aut}_{\bar{\mathbb{F}}_q}(E) \supsetneq \mu_4$ and it is easy to see that also in this case $\mathrm{Aut}_{\bar{\mathbb{F}}_q}((E, P)) = \{1\}$. We conclude that to every point $x \in X_1(3)(\mathbb{F}_q)$ not over $j = 0$ or ∞ there corresponds exactly one isomorphism class of pairs (E, P). Since $\# X_1(3)(\mathbb{F}_q) = q + 1$, we conclude that the number of isomorphism classes of pairs (E, P) equals

$$\sum_{\substack{j\text{-invariant} \\ \text{of } E \text{ is } 0}} \# H^1(\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q), \mathrm{Aut}_{\bar{\mathbb{F}}_q}((E, P))) + (q+1) - 2 - \begin{cases} 1 & \text{if } p = 2 \\ 2 & \text{if } p \neq 2. \end{cases}$$

Here the sum runs over the $\mathbb{F}_q$-isomorphism classes (E, P), where the j-invariant of E equals 0. It remains to evaluate this sum.

First, suppose that $p = 2$; in this case there is exactly one point in $X_1(3)(\mathbb{F}_q)$ over $j = 0$. If q is not a square it follows from Theorem (4.6) that there is only one supersingular curve E over $\mathbb{F}_q$ with a point of order 3. From Lemma (4.8) we see that $\# E(\mathbb{F}_q)[3] = 3$ and we conclude that upto isomorphism there is only one pair (E, P) over $\mathbb{F}_q$ with j-invariant of E equal to 0. If q is a square it follows from Theorem (4.6) that there are 3 supersingular curves E over $\mathbb{F}_q$ with a point of order 3. Two of them are in $I(-(\sqrt{q}/3)\sqrt{q})$ and these curves have $E(\mathbb{F}_q)[3]$ cyclic; the other is in $I(2(\sqrt{q}/3)\sqrt{q})$ and has $E(\mathbb{F}_q)[3] \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ by Lemma (4.8). This curve has all its endomorphisms defined over $\mathbb{F}_q$; this implies by Proposition (4.4)(i) that $\mathrm{Aut}_{\mathbb{F}_q}(E) = \mathrm{Aut}_{\bar{\mathbb{F}}_q}(E) \cong SL_2(\mathbb{F}_3)$ and this group acts transitively on the points of $E(\mathbb{F}_q)$ of order 3. We conclude that in this case there are exactly 3 isomorphism classes corresponding to the unique point in $X_1(3)(\mathbb{F}_q)$ over $j = 0$.

Next, suppose that $p \neq 2$. In this case there are two points over $j=0$. One has ramification index 1 and the other ramification index 3. Suppose (E, P) corresponds to the point x with ramification index 1: we have that $\mathbb{Z}[\zeta] \subset \mathrm{End}_{\bar{\mathbb{F}}_q}(E)$ and $P \in E(\mathbb{F}_q)$ is not annihilated by $\zeta - 1$. Since $p \neq 2$, we have that $\mathrm{Aut}_{\bar{\mathbb{F}}_q}(E) \subsetneq \mu_6$ and one shows easily that $\mathrm{Aut}_{\bar{\mathbb{F}}_q}((E, P)) = \{1\}$. This implies that the H^1 is trivial and that exactly one isomorphism class of pairs (E, P) corresponds to x. Finally, suppose that (E, P) corresponds to the point x over $j=0$ that has ramification index equal to 3. If $q \equiv -1 \pmod 3$ then E is supersingular and it follows from Proposition (4.4)(iii) that $\mathrm{Aut}_{\bar{\mathbb{F}}_q}(E) = \mu_6$; since P is annihilated by $\zeta - 1$ it follows that $\mathrm{Aut}_{\bar{\mathbb{F}}_q}((E, P)) = \mu_3$. We have that $\mathrm{Aut}_{\mathbb{F}_q}((E, P)) = \{1\}$ and a standard computation shows that $H^1(\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q), \mathrm{Aut}_{\bar{\mathbb{F}}_q}((E, P))) = H^1(\hat{\mathbb{Z}}, \mu_3) = 0$. If $q \equiv 1 \pmod 3$ we have that $\mathrm{Aut}_{\bar{\mathbb{F}}_q}((E, P)) = \mathrm{Aut}_{\mathbb{F}_q}((E, P)) = \mu_3$ with trivial action of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. We have that $H^1(\hat{\mathbb{Z}}, \mu_3) \cong \mathbb{Z}/3\mathbb{Z}$. We conclude that there are exactly $3 + (-3/q)$ isomorphism classes over $\mathbb{F}_q$ of pairs (E, P) corresponding to points in $X_1(3)(\mathbb{F}_q)$ over $j=0$. This proves the proposition.

(5.9) COROLLARY. *Let $\mathbb{F}_q$ be a finite field.*

(i) $$\sum_{t \in \mathbb{Z}} N(t) = 2q + 3 + 2\left(\frac{-3}{q}\right) + \left(\frac{-4}{q}\right).$$

(ii)
$$\sum_{t \in \mathbb{Z}} M(t) = 3q + \left(\frac{-4}{q}\right) \quad \text{if } q \equiv -1 \pmod 3,$$
$$= 3q + 2 + \left(\frac{-4}{q}\right) \quad \text{if } q \equiv 0 \pmod 3,$$
$$= 3q + 6 + \left(\frac{-4}{q}\right) \quad \text{if } q \equiv 1 \pmod 3.$$

Proof. The sum $\sum_t N(t)$ equals the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ and the sum $\sum_t M(t)$ equals the number of $\mathbb{F}_q$-isomorphism classes of pairs (E, P) with E an elliptic curve over $\mathbb{F}_q$ and P a point in $E(\mathbb{F}_q)$ [3]. The result follows from Propositions (5.7) and (5.8).

The formulas we obtain are in agreement with the ones given by Hirschfeld for every finite field $\mathbb{F}_q$ in [12, p. 315] columns n_0 and N or [13].

TABLE II

Cubic Curves over $\mathbb{F}_{16}$.

t	$q+1-t$	t^2-4q	$H(t^2-4q)$	$N(t)$	$N_3(t)$	$N_{3\times3}(t)$	$\varepsilon(t)$	$M(t)$
8	9			1	1	1	3	2
7	10	−15	2	2				2
6	11			0				0
5	12	−39	4	4	4			8
4	13			2				2
3	14	−55	4	4				4
2	15			0	0			0
1	16	−63	5	5				5
0	17			1				1
−1	18	−63	5	5	5	1		13
−2	19			0				0
−3	20	−55	4	4				4
−4	21			2	2			4
−5	22	−39	4	4				4
−6	23			0				0
−7	24	−15	2	2	2			4
−8	25			1				1
Σ				37				54

TABLE III

Cubic Curves over $\mathbb{F}_{25}$

t	$q+1-t$	t^2-4q	$H(t^2-4q)$	$N(t)$	$N_3(t)$	$N_{3\times3}(t)$	$\varepsilon(t)$	$M(t)$
10	16			1				1
9	17	−19	1	1				1
8	18	−36	3	3	3	1	2	7
7	19	−51	2	2				2
6	20	−64	4	4				4
5	21			2	2			4
4	22	−84	4	4				4
3	23	−91	2	2				2
2	24	−96	6	6	6			12
1	25	−99	3	3				3
0	26			0				0
−1	27	−99	3	3	3	1		9
−2	28	−96	6	5				6
−3	29	−91	2	2				2
−4	30	−84	4	4	4			8
−5	31			2				2
−6	32	−64	4	4				4
−7	33	−51	2	2	2			4
−8	34	−36	3	6				6
−9	35	−19	1	1				3
−10	36			1	1	1	2	3
Σ				56				82

TABLE IV

Cubic Curves over $\mathbb{F}_{27}$

t	$q+1-t$	t^2-4q	$H(t^2-4q)$	$N(t)$	$N_3(t)$	$N_{3\times 3}(t)$	$\varepsilon(t)$	$M(t)$
10	18	−8	1	1	1			2
9	19			1				1
8	20	−44	4	4				4
7	21	−59	3	3	3			6
6	22			0				0
5	23	−83	3	3				3
4	24	−92	6	6	6			12
3	25			0				0
2	26	−104	6	6				6
1	27	−107	3	3	3			6
0	28			2				2
−1	29	−107	3	3				3
−2	30	−104	6	6	6			12
−3	31			0				0
−4	32	−92	6	6				6
−5	33	−83	3	3	3			6
−6	34			0				0
−7	35	−59	3	3				3
−8	36	−44	4	4	4			8
−9	37			1				1
−10	38	−8	1	1				1
Σ				56				82

$\mathrm{End}_{\mathbb{F}_q}(E)=\mathcal{O}(-63)$ and one has $\mathrm{End}_{\mathbb{F}_q}(E)=\mathcal{O}(-7)$; the latter curve has nine 3-torsion points in $E(\mathbb{F}_q)[3]$.

In Table III we have that $t_0=-10$ and $t_1=8$. There are precisely three curves E with $E(\mathbb{F}_q)[3]$ of order 9. One has $\#E(\mathbb{F}_q)=18$ and $\mathrm{End}_{\mathbb{F}_q}(E)=\mathbb{Z}[i]$; one has $\#E(\mathbb{F}_q)=27$ and $\mathrm{End}_{\mathbb{F}_q}(E)=\mathcal{O}(-11)$; the last one is supersingular; it has $\#E(\mathbb{F}_q)=36$ and $E(\mathbb{F}_q)\cong\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}$; its ring of $\mathbb{F}_q$-endomorphisms is the maximal order in $\mathbb{Q}_{\infty,5}$.

ACKNOWLEDGMENTS

I thank James Hirschfeld for his interest in this work and Hendrik Lenstra for suggesting the proof of Proposition (5.4).

REFERENCES

1. E. BEDOCCHI, Classi di isomorfismo delle cubiche di $\mathbb{F}_q$, *Rendic. Circ. Mat. Palermo. Ser. 2* **30** (1981), 397–415.

2. Z. BOREVIC AND I. ŠAFAREVIČ, "Number Theory," Academic Press, London/New York, 1966.
3. D. A. BUELL, Class groups of quadratic fields II, *Math. Comp.* **48** (1987), 85–93.
4. M. CICCHESE, Sulle cubiche di un piano di Galois, *Rend. Mat.* (3–4), **24** (1965), 291–330.
5. M. CICCHESE, Sulle cubiche di un piano lineare $S_{2,q}$ con $q \equiv 1 \pmod 3$, *Rend. Mat.* (2) **4** (1971), 349–383.
6. R. DE GROOTE AND J. HIRSCHFELD, The number of points on an elliptic cubic curve over a finite field, *Europ. J. Combin.* **1** (1980), 327–333.
7. P. DELIGNE AND M. RAPOPORT, Schémas de modules de courbes elliptiques, *in* "Lecture Notes in Mathematics," Vol. 349, Springer–Verlag, Berlin/Heidelberg/New York, 1973.
8. M. DEURING, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Univ. Hamburg* **14** (1941), 197–272.
9. M. DEURING, Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primer Grundzahl, *Jahresber. Deutsch. Math.–Verein* **54** (1951), 24–41.
10. C. F. GAUSS, "Disquisitiones Arithmeticae," Leipzig 1801, Vol. I of Gauss Werke, Göttingen, 1870.
11. R. HARTSHORNE, "Algebraic Geometry," Springer–Verlag, Berlin/Heidelberg/New York, 1977.
12. J. HIRSCHFELD, "Projective Geometries over Finite Fields," Oxford Univ. Press (Clarendon), Oxford, 1979.
13. J. HIRSCHFELD, The Weil conjectures in finite geometry, *in* "Proc. Australian Conf. Combinatoric Math. Adelaide, 1982," Lecture Notes in Mathematics, Vol. 1036, Springer–Verlag, Berlin/Heidelberg/New York, 1983.
14. J. P. SERRE, "Corps Locaux," Hermann, Paris, 1968.
15. G. SHIMURA, "Introduction to the Arithemtic of Automorphic Functions," Iwanami Shoten, Princeton Univ. Press. Princeton, NJ, 1971.
16. J. TATE, Endomorphisms of abelian varieties over finite fields, *Invent. Math.* **2** (1966), 134–144.
17. J. TATE, The arithmetic of elliptic curves, *Invent. Math.* **23** (1974), 179–206.
18. E. UGHI, On the number of points of elliptic curves over finite fields and a problem of B. Serge, *Europ. J. Combin.* **4** (1983), 263–270.
19. E. WATERHOUSE, Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup.* **2** (1969), 521–560.

Printed by Catherine Press, Ltd., Tempelhof 41, B-8000 Brugge, Belgium

6. Class Numbers and Examples

In this section we give a table of Kronecker class numbers as defined in Section 2 (see Table I).

Finally we compute the function $M(t)$ for some small fields $\mathbb{F}_q$. By Proposition (3.6)(ii) and the remark after the proof of Theorem (5.2) we have that $M(t)=0$ whenever $|t|>2\sqrt{q}$. We use Theorem (4.6) and Table I to compute $N(t)$. The value of $N_3(t)$ follows easily from the value of t: the number $N_3(t)$ equals $N(t)$ if $t\equiv q+1 \pmod 3$ and $N_3(t)$ equals 0 otherwise. We compute $N_{3\times 3}(t)$ using Theorem (4.9) and the table of class numbers. The values of $M(t)$ follow easily from Theorem (5.2). The values of $\sum_t N(t)$ and $\sum_t M(t)$ that we obtain are in agreement with the ones given in Corollary (5.9). In Table II $t_0=t_1=8$ and hence $\varepsilon(8)=3$. In $I(-1)$ there are 5 isomorphism classes of curves E; four of them have

TABLE I

$-\Delta$	$H(\Delta)$	$-\Delta$	$H(\Delta)$	$-\Delta$	$H(\Delta)$	$-\Delta$	$H(\Delta)$
3	1	52	2	103	5	152	6
4	1	55	4	104	6	155	4
7	1	56	4	107	3	156	8
8	1	59	3	108	6	159	10
11	1	60	4	111	8	160	6
12	2	63	5	112	4	163	1
15	2	64	4	115	2	164	8
16	2	67	1	116	6	167	11
19	1	68	4	119	10	168	4
20	2	71	7	120	4	171	5
23	3	72	3	123	2	172	4
24	2	75	3	124	6	175	7
27	2	76	4	127	5	176	10
28	2	79	5	128	7	179	5
31	3	80	6	131	5	180	6
32	3	83	3	132	4	183	8
35	2	84	4	135	8	184	4
36	3	87	6	136	4	187	2
39	4	88	2	139	3	188	10
40	2	91	2	140	8	191	13
43	1	92	6	143	10	192	8
44	4	95	8	144	8	195	4
47	5	96	6	147	3	196	5
48	4	99	3	148	2	199	9
51	2	100	3	151	7	200	7