

# Cubic Curves, Finite Geometry and Cryptography

A.A. Bruen, J.W.P. Hirschfeld, and D.L. Wehlau

## Abstract

Some geometry on non-singular cubic curves, mainly over finite fields, is surveyed. Such a curve has 9, 3, 1 or 0 points of inflexion, and cubic curves are classified accordingly. The group structure and the possible numbers of rational points are also surveyed. A possible strengthening of the security of elliptic curve cryptography is proposed using a ‘shared secret’ related to the group law. Cubic curves are also used in a new way to construct sets of points having various combinatorial and geometric properties that are of particular interest in finite Desarguesian planes.

Keywords: Cubic curves, group law, non-singularity, elliptic curve cryptography, finite geometries

## 1 Introduction

In cryptography, the following views of an elliptic curve over a particular field  $K$  are common:

- (i) a curve of genus 1;
- (ii) a plane non-singular cubic curve;
- (iii) a plane non-singular cubic curve with an inflexion;
- (iv)  $\{(x, y) \mid y^2 = x^3 + ax + b\}$ .

In this paper (iii) is used; for many fields, it is equivalent to (iv).

However, to perform elliptic curve cryptography (ECC) on a non-singular cubic curve it is really not necessary to assume that the curve has an inflexion. This then widens the choice of the curve that is used for the encryption. If only non-singular cubics with more than one inflexion point are considered then, since an inflexion point other than the zero has order 3 and the order of a subgroup divides the order of the group, this restricts to curves whose group size is divisible by 3.

Given two irreducible curves  $\mathcal{C}$ ,  $\mathcal{D}$ , an *isomorphism* from  $\mathcal{C}$  to  $\mathcal{D}$  is an invertible polynomial transformation; it induces an isomorphism of their function fields. A non-singular

cubic curve is isomorphic to one containing at least one inflexion point; see, for example, [6, Section 7.10]. Two non-singular cubics, both with at least one inflexion, are isomorphic if and only if there is a projective transformation between them. So to classify non-singular cubics up to isomorphism is equivalent to classifying non-singular cubics with an inflexion up to projective transformation.

Given a non-singular cubic with an inflexion, when the field  $K$  has characteristic other than two, co-ordinates may be chosen so that the line at infinity contains an inflexion point and the curve is normalised to the form  $y^2 = f(x)$ , where  $f$  has degree 3. Canonical forms for these cubics are given in Section 6.3. However, there do exist non-singular cubic curves having no inflexion point; see Section 6.4.

Also, in this paper, a modification of the usual version of elliptic curve cryptography is suggested. Suppose two parties  $A$  and  $B$  are establishing a secret key using elliptic curve cryptography. They are working with a given cubic curve  $\mathcal{C}$ ; it may be singular or non-singular and it may or may not have an inflexion. It may also be noted that elliptic curve cryptography may be carried out over any finite field using any cubic curve. In the usual version of elliptic curve cryptography, the line at infinity is a tangent at the inflexion  $O = (0 : 1 : 0)$ . The identity element for the group structure is always chosen to be the inflexion point  $O$ . In the proposed variation,  $A$  and  $B$  share a secret. This secret, which will be digitised, is the choice of the identity element which is known only to  $A$  and  $B$  and which can be any point of the curve  $\mathcal{C}$ . The choice of this identity point determines the group operation. The unknown identity of the identity point then makes the task of an eavesdropper that much more difficult.

In Section 8, some new and purely geometrical applications of cubic curves over finite fields are discussed.

## 2 Projective plane curves

Let  $K$  be any field and let  $\overline{K}$  be its algebraic closure. Let  $F(X, Y, Z)$  be a form, that is, a homogeneous polynomial in  $K[X, Y, Z]$ . The graph of this form,

$$\mathcal{C} = \{(x : y : z) \in \mathbf{P}^2(K) \mid F(x, y, z) = 0\},$$

is a *curve* in the projective plane  $\mathbf{P}^2(K)$ . The curve is *irreducible* if  $F(X, Y, Z)$  does not factor in  $\overline{K}[X, Y, Z]$ .

A point  $P$  lying on a curve is a *singular point* of the curve if there is more than one tangent line to the curve through  $P$ , [6, Section 1.3]. If no such point exists in  $\mathbf{P}^2(\overline{K})$ , that is, if there is a unique tangent line at each point of the curve considered over  $\overline{K}$ , then the curve is *non-singular*. This means that, working over the algebraic closure of  $K$ , it is impossible to find a point  $P$  on  $\mathcal{C}$  such that the three partial derivatives of  $F$  with respect to  $X, Y, Z$  are all zero at  $P$ . If a curve  $\mathcal{C}$  in  $\mathbf{P}^2(K)$  has a singular point in  $\mathbf{P}^2(\overline{K})$  then the curve  $\mathcal{C}$  is *singular*.

Geometrically, the non-singularity of  $\mathcal{C}$  means that it has no node or cusp or isolated double point; so there is a unique tangent line to the curve at every point  $P$ .

### 3 Inflexion points

A *point of inflexion*  $P$  of a curve is one for which the tangent at  $P$  has triple contact with the curve, [6, Section 1.3]. Thus, in particular, the tangent line at an inflexion  $P$  of a cubic curve has no other point in common with the curve.

The condition that the tangent line at  $P$  has triple contact with the curve is expressed algebraically by the requirement that

$$F(X, Y, Z) = f(X, Y, Z) \cdot g(X, Y, Z) + (aX + bY + cZ)^3 h(X, Y, Z),$$

where

- (i)  $f(X, Y, Z)$  is the linear form defining the tangent line at  $P$ ,
- (ii)  $g(X, Y, Z)$  is some form of degree  $n - 1$ ,
- (iii)  $h(X, Y, Z)$  is a form of degree  $n - 3$ ,
- (iv)  $aX + bY + cZ$  is some linear form vanishing at  $P$ ,
- (v)  $n$  is the degree of the form  $F$ .

For cubic curves, Points of inflexion are considered in relation to the group structure in Section 4.

Over any field, the line joining any two inflexions meets the cubic in a third inflexion. To see this result the following Theorem of the Nine Associated Points is used.

**Theorem 3.1.** *Let  $\mathcal{E}$  be an irreducible cubic curve defined over  $K$  by  $E$  and suppose that  $\mathcal{D}$  and  $\mathcal{D}'$  are any two other cubic curves defined over  $K$  by the forms  $D$  and  $D'$ . If*

$$\begin{aligned}\mathcal{E} \cdot \mathcal{D} &= P_1 + P_2 + \cdots + P_9, \\ \mathcal{E} \cdot \mathcal{D}' &= P_1 + P_2 + \cdots + P_8 + R,\end{aligned}$$

then  $R = P_9$ .

**Proof** Here, the classical proof is given in the case that the  $P_i$  are distinct. The general proof follows from Noether's Theorem; see Fulton [4, Section 5.6] or [6, Section 4.5]. The general cubic form  $F(X, Y, Z)$  has 10 coefficients. The 8 equations  $E(P_i) = 0$  for  $i = 1, 2, \dots, 8$  impose 8 linearly independent conditions on the form  $E$ . So there is a pencil of cubics which pass through the 8 points  $P_1, P_2, \dots, P_8$ . Hence  $D' = \alpha E + \beta D$  for some  $\alpha, \beta \in K$ . Since  $E(P_9) = D(P_9) = 0$ , so  $D'(P_9) = 0$ . Therefore  $R = P_9$ .  $\square$

**Theorem 3.2.** *Let  $\mathcal{C}$  be a cubic defined over  $K$ . If  $P_1, P_2$  are two distinct inflexion points of  $\mathcal{C}$  lying in  $\mathbf{P}^2(K)$ , and the line  $\ell = P_1P_2$  meets  $\mathcal{C}$  again in  $P_3$ , then  $P_3$  is also an inflexion point of  $\mathcal{C}$ .*

**Proof** Let  $\ell_i$  be the tangent line to  $\mathcal{C}$  at the point  $P_i$ ,  $i = 1, 2, 3$ , and let  $\mathcal{C} \cdot \ell_3 = 2P_3 + R$ . Define two cubics  $\mathcal{D} = \ell^3$  and  $\mathcal{D}' = \ell_1\ell_2\ell_3$ . Then

$$\begin{aligned}\mathcal{C} \cdot \mathcal{D} &= 3P_1 + 3P_2 + 3P_3, \\ \mathcal{C} \cdot \mathcal{D}' &= 3P_1 + 3P_2 + 2P_3 + R.\end{aligned}$$

So, by the previous theorem,  $R = P_3$ ; that is,  $\mathcal{C} \cdot \ell_3 = 3P_3$  and thus  $P_3$  is an inflexion point of  $\mathcal{C}$ .  $\square$

Given a form  $F(x, y, z)$  of degree  $n$ , its *Hessian*  $\mathcal{H}$  is defined as the curve given by the form  $H$  that is the determinant of the second-order partial derivatives of  $F$ :

$$H = \begin{vmatrix} F_{XX} & F_{XY} & F_{XZ} \\ F_{YX} & F_{YY} & F_{YZ} \\ F_{ZX} & F_{ZY} & F_{ZZ} \end{vmatrix}.$$

Thus the Hessian is a curve of degree  $3(n - 2)$ .

**Theorem 3.3.** *Suppose  $F(X, Y, Z) \in K[X, Y, Z]$  is a form of degree  $n$  and that  $2(n - 1)$  is invertible in  $K$ . A non-singular point  $P$  lying on the curve  $\mathcal{C}$  defined by  $F$  is an inflexion point of  $\mathcal{C}$  if and only if its Hessian form  $H$  vanishes at  $P$ .*

**Remark 3.4.** If  $2(n - 1)$  is not invertible in  $K$  then  $H$  is identically zero. For an appropriate treatment in this case, see [5, Section 11.2].

Suppose now that  $\mathcal{C}$  is a non-singular cubic curve. Then its Hessian  $\mathcal{H}$  is also a cubic. Bézout's Theorem shows that, over an algebraically closed field of characteristic different from 2 and 3, there are, in general, 9 inflexion points of  $\mathcal{C}$ .

Over the field of complex numbers these nine points form a famous configuration, namely the 9 points of  $\text{AG}(2, 3)$ , the affine plane of order 3. Classically this  $(9_4, 12_3)$  configuration of 9 points and 12 lines, with 4 lines through a point and 3 points on a line, is called the Hesse Configuration. Over a finite field  $K = \mathbf{F}_q$  there are 0, 1, 3 or 9 inflexions. In the case of 9 inflexions, the 9 points again form a copy of  $\text{AG}(2, 3)$  embedded in the projective plane  $\text{PG}(2, q)$ .

**Theorem 3.5.** *The number of rational inflexions of a non-singular cubic over  $\mathbf{F}_q$  is 0, 1, 3, or 9. The possibilities are as follows:*

$$\begin{aligned}q \equiv 0 \pmod{3} &: & 0, 1, 3; \\ q \equiv 2 \pmod{3} &: & 0, 1, 3; \\ q \equiv 1 \pmod{3} &: & 0, 1, 3, 9.\end{aligned}$$

In the case that  $q \equiv 1 \pmod{3}$ , by a suitable choice of coordinates, the configuration of 9 points always has the following form  $\mathcal{K}_9$ , where  $\omega$  is a primitive cube root of unity in  $K$ :

$$\begin{aligned} \mathcal{K}_9 = \{ & (0, 1, -1), (0, 1, -\omega), (0, 1, -\omega^2), (-1, 0, 1), (-\omega, 0, 1), \\ & (-\omega^2, 0, 1), (1, -1, 0), (1, -\omega, 0), (1, -\omega^2, 0) \} \end{aligned} \quad (3.1)$$

This set  $\mathcal{K}_9$  is a Hessian configuration for the non-singular cubic with form

$$F = X^3 + Y^3 + Z^3 - 3cXYZ,$$

with  $c$  any element such that  $c^3 \neq 1$ . When  $q = 4$ , take  $c = 0$ ; then  $\mathcal{K}_9$  is the set of rational points of the Hermitian curve with form

$$X\bar{X} + Y\bar{Y} + Z\bar{Z},$$

where  $\bar{T} = T^{\sqrt{q}} = T^2$ .

For further illumination on inflexions of a cubic, including the singular ones, see [5, Chapter 11].

The advent of elliptic curve cryptography has aroused considerable interest in elliptic curves over  $\mathbf{F}_q$ . The main idea involves a key-exchange between two communicating parties, similar to the Diffie–Hellman protocol. There is a publicly prescribed elliptic curve over some finite field, with associated group  $G$  that may be taken to be cyclic, with generator  $P$ . Communicating parties  $A, B$  choose their secret positive numbers  $\alpha, \beta$ . Then  $A$  openly transmits the point  $\alpha P$ , that is,  $P$  added to itself  $\alpha$  times, to  $B$ . Also,  $B$  transmits  $\beta P$  in the open to  $A$ . Now,  $A$  calculates  $\alpha(\beta P)$  and  $B$  calculates  $\beta(\alpha P)$ . The upshot is that  $A$  and  $B$  are now in possession of a common secret key  $\alpha\beta P = \beta\alpha P$ . Security rests on the unproved assumption that, given  $mP$ , it is not possible to calculate  $m$  in a ‘reasonable’ amount of time. The commercialisation of this key-exchange has led to an intensive study of elliptic curves over a finite field.

## 4 The group law on a cubic

Let  $\mathcal{C}$  be an irreducible cubic curve in  $\mathbf{P}^2(K)$ , and consider only the *rational* points of  $\mathcal{C}$ , that is, those lying over  $K$ ; denote this set by  $\mathcal{C}(K)$ . If  $\mathcal{C}$  is singular with singularity  $P_0$ , let  $\mathcal{C}(K)' = \mathcal{C}(K) \setminus \{P_0\}$ . When  $\mathcal{C}$  is non-singular, write  $\mathcal{C}(K)' = \mathcal{C}(K)$ .

If  $P, Q$  are points of  $\mathcal{C}(K)'$  then define  $P * Q$  to be the third intersection of the line  $PQ$  with  $\mathcal{C}$ . In particular, when  $Q = P$ , the line  $PQ$  is the tangent at  $P$  and  $P * P = P_t$  is the *tangential* of  $P$ . If  $P$  is an inflexion then  $P_t = P$ .

Now choose any point  $O$  of  $\mathcal{C}(K)'$  as the identity point for the group operation. Then an operation  $\oplus$  is defined on  $\mathcal{C}(K)'$  as follows:

$$P \oplus Q = (P * Q) * O. \quad (4.1)$$

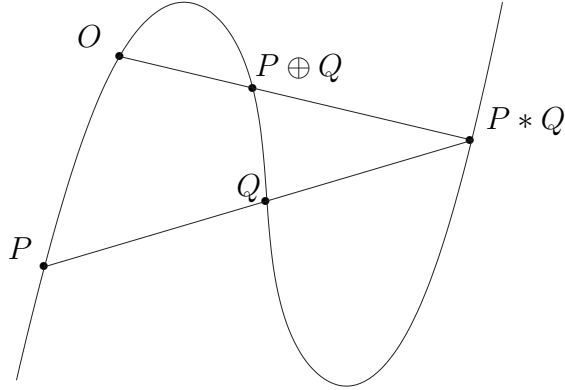


Figure 1: Abelian group law on an elliptic curve

The negative of  $\oplus$  is written  $-$ .

Let the tangential  $O_t$  at  $O$  be denoted by  $N$ .

**Theorem 4.1.** (i) *The points of  $\mathcal{C}(K)'$  form a group  $G$  with identity  $O$  under the operation  $\oplus$ .*

(ii)  $-N = N$ .

(iii) *Three points  $P, Q, R$  of  $\mathcal{C}(K)'$  are collinear if and only if  $P \oplus Q \oplus R = N$ .*

(iv) *If  $O$  is an inflexion, then three points  $P, Q, R$  of  $\mathcal{C}(K)'$  are collinear if and only if  $P \oplus Q \oplus R = O$ .*

If the characteristic of  $K$  is not 2 or 3, then, as in Theorem 6.4,  $\mathcal{C}$  may be given by the form  $F = Y^2Z - X^3 - cXZ^2 - dZ^3$ .

With the identity point  $O = (0 : 1 : 0)$  the group law may be expressed algebraically as follows. With  $P = (x_1 : y_1 : 1)$  and  $Q = (x_2 : y_2 : 1)$ ,

$$P \oplus Q = \begin{cases} (0 : 1 : 0), & \text{if } x_1 = x_2 \text{ and } y_1 \neq y_2, \\ (\gamma^2 - x_1 - x_2 : -\gamma^3 + 2\gamma x_1 + \gamma x_2 - y_1 : 1), & \text{otherwise,} \end{cases}$$

where

$$\gamma = \begin{cases} 3x_1^2 + a/(2y_1), & \text{if } x_1 = x_2, \\ (y_2 - y_1)/(x_2 - x_1), & \text{if } x_1 \neq x_2; \end{cases}$$

see [3, Section 6.6].

Part (iii) of Theorem 4.1 can be generalised to curves of higher degree.

**Theorem 4.2.** (i) *The six distinct points  $P, Q, R, S, T, U$  of  $\mathcal{C}(K)'$  lie on a conic if and only if  $P \oplus Q \oplus R \oplus S \oplus T \oplus U = 2N$ .*

- (ii) A set of  $3m$  points  $P_1, P_2, \dots, P_{3m}$  of  $\mathcal{C}(K)'$  lie on a curve of order  $m$  if and only if  $\sum_{i=1}^m P_i = mN$ .

For cubics, geometric results have algebraic counterparts. Here is a sample from [7], originally for the complex numbers, but applicable over any field.

Geometric formulation	Group-theoretic formulation
$P$ and $Q$ have the same tangential	$2P = 2Q$ or $2(P - Q) = 0$
There exist four tangents from $P$	$2X \oplus P = N$ has four solutions
$P$ is a inflexion	$3P = N$
$\mathcal{C}$ has 9 inflexions	$3P = N$ has nine solutions
If $P$ and $Q$ are inflexions then $R = P * Q$ is another inflexion; if $P \neq Q$ then $R \neq P, Q$	If $3P = N$ and $3Q = N$ , then $P \oplus Q \oplus R = N$ implies $3R = N$

The calculations become more familiar, but not less complicated, if the point  $O$  is in fact an inflexion point. It is important to note that all different choices for  $O$  yield isomorphic groups.

## 5 Classification of singular cubics

An irreducible cubic  $\mathcal{C}$  over  $K$  with a singular point  $P_0$  has 2, 1 or 0 tangents lying over  $K$  at  $P_0$ , which is correspondingly a *node*, *cusp* or *isolated double point*. Let  $\mathcal{N}_i^j$  indicate an irreducible singular cubic over  $\mathbf{F}_q$  with  $i$  rational inflexions and  $j$  distinct rational tangents at the singularity; here, ‘rational’ means ‘over  $K$ ’.

When the characteristic of  $K$  is 3, there is one cubic  $\mathcal{C} = \mathcal{N}_q^1$  of particular note. It has the associated canonical form  $F = ZY^2 - X^3$  and every point of  $\mathcal{N}_q^1$  in  $\mathbf{P}^2(K)$  other than the singular point  $P_0 = (0 : 0 : 1)$  is an inflexion.

**Theorem 5.1.** (i) For an irreducible singular plane cubic curve  $\mathcal{C}$  over  $\mathbf{F}_q$ , with  $\mathcal{C} \neq \mathcal{N}_q^1$ ,

- (a) there are 3 collinear inflexions over  $\overline{K}$ ;
- (b) the inflexions are rational or lie over a quadratic extension or a cubic extension.

- (ii) For any  $q$  there are precisely four projectively distinct singular cubics.

In Table 1, canonical forms are given in the cases of a node and a cusp including  $\mathcal{N}_q^1$ . For the canonical forms in the case of an isolated double point, see [5, Section 11.4].

Table 1: Canonical forms for singular cubics

Symbol	$q \equiv m \pmod{12}$ $m$	Form
$\mathcal{N}_1^2$	3, 9, 2, 8, 5, 11	$XYZ - X^3 - Y^3$
$\mathcal{N}_3^2$	4, 1, 7	$XY - X^3 - Y^3$
$\mathcal{N}_0^2$	4, 1, 7	$XYZ - X^3 - \alpha Y^3$ , $\alpha$ non-cube
$\mathcal{N}_0^1$	3, 9	$ZY^2 - X^2Y - X^3$
$\mathcal{N}_q^1$	3, 9	$ZY^2 - X^3$
$\mathcal{N}_1^1$	2, 8, 4, 1, 5, 7, 11	$ZY^2 - X^3$

There is a nice combinatorial/geometric characterisation of singular cubics due to Tallini Scafati [11]. See also [5, Section 12.8].

**Theorem 5.2.** *Let  $\mathcal{K}$  be a set of  $k$  points in  $\text{PG}(2, q)$ , with  $q$  odd,  $q > 11$ , and with no 4 points of  $\mathcal{K}$  collinear. If  $\mathcal{K}$  contains 4 points  $P, P_1, P_2, P_3$  such that*

- (i) *there is no line through  $P$  intersecting  $\mathcal{K}$  in 3 points,*
- (ii) *any conic through  $P$  and one of the  $P_i$  meets  $\mathcal{K}$  in at most 3 other points,*
- (iii)  $k > q - \frac{1}{4}\sqrt{q} + \frac{19}{4}$ ,

*then  $\mathcal{K}$  is contained in a rational cubic with a double point at  $P$ .*

Due to later results, see [5, Sections 10.4, 10.5] the lower bound in (iii) in this theorem can be improved.

## 6 Classification of non-singular cubics

The following result from Section 3 is recalled.

**Theorem 6.1.** *If  $\mathcal{C}$  is a non-singular cubic curve defined over  $K$  then  $\mathcal{C}$  has exactly 0, 1, 3 or 9 inflexion points in  $\mathbf{P}^2(K)$ .*



## 6.1 Non-singular cubics with nine rational inflexions

**Theorem 6.2.** *A non-singular cubic  $\mathcal{C}$  with form  $F$  and nine rational inflexions exists over  $\mathbf{F}_q$  if and only if  $q \equiv 1 \pmod{3}$ , and then  $F$  has canonical form*

$$F = X^3 + Y^3 + Z^3 - 3cXYZ.$$

The nine inflexions are those given in (3.1).

## 6.2 Non-singular cubics with three rational inflexions

**Theorem 6.3.** *A non-singular cubic  $\mathcal{C}$  with form  $F$  and three rational inflexions exists over  $\mathbf{F}_q$  for all  $q$ . The inflexions are necessarily collinear.*

(i) *If the inflexional tangents are concurrent, the canonical forms are as follows:*

(a)  $q \equiv 0, 2 \pmod{3}$ ,

$$F = XY(X + Y) + Z^3;$$

(b)  $q \equiv 1 \pmod{3}$ ,

$$\begin{aligned} F &= XY(X + Y) + Z^3, \\ F &= XY(X + Y) + \alpha Z^3, \\ F &= XY(X + Y) + \alpha^2 Z^3, \end{aligned}$$

where  $\alpha$  is a primitive element of  $\mathbf{F}_q$ .

(ii) *If the inflexional tangents are non-concurrent, the canonical form is as follows:*

$$F = XYZ + e(X + Y + Z)^3,$$

$$e \neq 0, -1/27.$$

In case (i), the inflexions are

$$(1 : 0 : 0), (0 : 1 : 0), (1 : -1 : 0);$$

in case (ii), the inflexions are

$$(0 : 1 : -1), (1 : 0 : -1), (1 : -1 : 0).$$

### 6.3 Non-singular cubics with one rational inflexion

For  $q = 2^h$ , the *trace* of an element  $x \in \mathbf{F}_q$  is

$$\tau(x) = x + x^2 + x^4 + \cdots + x^{2^{h-1}}.$$

**Theorem 6.4.** *A non-singular, plane, cubic curve defined over  $\mathbf{F}_q$ ,  $q = p^h$ , with at least one inflexion has one of the following canonical forms  $F$ .*

(i)  $p \neq 2, 3$ ,

$$F = Y^2Z - X^3 - cXZ^2 - dZ^3,$$

where  $4c^3 + 27d^2 \neq 0$ .

(ii)  $p = 3$ ,

(a)

$$F = Y^2Z - X^3 - bX^2Z - dZ^3,$$

where  $bd \neq 0$ ;

(b)

$$F' = Y^2Z - X^3 - cXZ^2 - dZ^3,$$

where  $c \neq 0$ .

(iii)  $p = 2$ ,

(a)

$$F = Y^2Z + XYZ + X^3 + bX^2Z + dZ^3,$$

where  $b = 0$  or a fixed element of trace 1, and  $c \neq 0$ ;

(b)

$$F = Y^2Z + YZ^2 + eX^3 + cXZ^2 + dZ^3,$$

where  $e = 1$  when  $q \equiv 0, 2 \pmod{3}$  and  $e = 1, \alpha, \alpha^2$  when  $q \equiv 1 \pmod{3}$ , with  $\alpha$  a primitive element of  $\mathbf{F}_q$ ; also,  $d = 0$  or a given element of trace 1.

A complete discussion and classification of cubic curves over finite fields may be found in [5].

### 6.4 Non-singular cubics with no rational inflexions

**Theorem 6.5.** *A non-singular, plane, cubic curve defined over  $\mathbf{F}_q$ ,  $q = p^h$ , with no rational inflexion has one of the following canonical forms  $F$ .*

(i)  $q \equiv 2 \pmod{3}$ ,

$$F = Z^3 - 3c(X^2 - dXY + Y^2)Z - (X^3 - 3XY^2 + dY^3),$$

where  $T^3 - 3T + d$  is irreducible.

(ii)  $q \equiv 1 \pmod{3}$ ,

(a)

$$F = X^3 + \alpha Y^3 + \alpha^2 Z^3 - 3cXYZ,$$

with  $\alpha$  a primitive element of  $\mathbf{F}_q$ .

(b)

$$F = XY^2 + X^2Z + eYZ^2 - c(X^3 + eY^3 + e^2Z^3 - 3eXYZ),$$

with  $\alpha$  a primitive element of  $\mathbf{F}_q$  and  $e = \alpha, \alpha^2$ .

(ii)  $q \equiv 0 \pmod{3}$ ,

$$F = X^3 + Y^3 + cZ^3 + dX^2Z + dXY^2 + d^2X^2 + dYZ^2,$$

where  $c \neq 1$  and  $T^3 + dT - 1$  is a fixed irreducible polynomial.

## 7 Number of rational points on a cubic

With  $N_1$  the number of rational points on a curve  $\mathcal{F}$ , consider the case that  $\mathcal{F}$  is a non-singular plane cubic  $\mathcal{C}$ . The Hasse bound states that

$$q + 1 - 2\sqrt{q} \leq N_1 \leq q + 1 + 2\sqrt{q}. \quad (7.1)$$

The next result shows what values in the range actually occur. For any integer  $M$  and any prime divisor  $\ell$ , let  $v_\ell(M)$  be the highest power of  $\ell$  dividing  $M$ ; that is,  $\prod_\ell \ell^{v_\ell(M)}$  is the prime decomposition of  $M$ .

**Theorem 7.1.** *There exists a non-singular plane cubic over  $\mathbf{F}_q$ ,  $q = p^h$ , with precisely  $N_1 = q + 1 - t$  rational points, where  $|t| \leq 2\sqrt{q}$ , in the cases listed in Table 2. Below,  $G_{\mathcal{C}}$  is the corresponding group formed by the points of the cubic.*

$$(1) \quad G_{\mathcal{C}} = \mathbf{Z}/(p^{v_p(N_1)}) \times \prod_{\ell \neq p} (\mathbf{Z}/(\ell^{r_\ell}) \times \mathbf{Z}/(\ell^{s_\ell})),$$

with  $r_\ell + s_\ell = v_\ell(N_1)$  and  $\min(r_\ell, s_\ell) \leq v_\ell(q - 1)$ ;

$$(2) \quad G_{\mathcal{C}} = \begin{cases} \mathbf{Z}/(q + 1) & \text{for } q \not\equiv -1 \pmod{4}, \\ \mathbf{Z}/(q + 1) \text{ or } \mathbf{Z}/(2) \times \mathbf{Z}/((q + 1)/2) & \text{for } q \equiv -1 \pmod{4}; \end{cases}$$

$$(4) \quad G_{\mathcal{C}} = \mathbf{Z}/(N_1);$$

Table 2: Values of  $t$

	$t$	$p$	$h$
(1)	$t \not\equiv 0 \pmod{p}$		
(2)	$t = 0$		<i>odd</i>
(3)	$t = 0$	$p \not\equiv 1 \pmod{4}$	<i>even</i>
(4)	$t = \pm\sqrt{q}$	$p \not\equiv 1 \pmod{3}$	<i>even</i>
(5)	$t = \pm 2\sqrt{q}$		<i>even</i>
(6)	$t = \pm\sqrt{2q}$	$p = 2$	<i>odd</i>
(7)	$t = \pm\sqrt{3q}$	$p = 3$	<i>odd</i>

(5)  $G_{\mathcal{C}} = \mathbf{Z}/(\sqrt{N_1}) \times \mathbf{Z}/(\sqrt{N_1})$ ,  $N_1 = (\sqrt{q} \pm 1)^2$ ;

(6)  $G_{\mathcal{C}} = \mathbf{Z}/(N_1)$ ;

(7)  $G_{\mathcal{C}} = \mathbf{Z}/(N_1)$ .

The range of  $t$  is due to Waterhouse [14] and the corresponding groups independently to Rück [8] and Voloch [13].

Let  $N_q(1)$  denote the maximum number of rational points on any non-singular cubic over  $\mathbf{F}_q$  and  $L_q(1)$  the minimum number. The prime power  $q = p^h$  is *exceptional* if  $h$  is odd,  $h \geq 3$ , and  $p$  divides  $\lfloor 2\sqrt{q} \rfloor$ .

**Corollary 7.2.** *The bounds  $N_q(1)$  and  $L_q(1)$  are as follows:*

(i)  $N_q(1) = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor, & \text{if } q \text{ is exceptional} \\ q + 1 + \lfloor 2\sqrt{q} \rfloor, & \text{if } q \text{ is non-exceptional;} \end{cases}$

(ii)  $L_q(1) = \begin{cases} q + 2 - \lfloor 2\sqrt{q} \rfloor, & \text{if } q \text{ is exceptional} \\ q + 1 - \lfloor 2\sqrt{q} \rfloor, & \text{if } q \text{ is non-exceptional.} \end{cases}$

**Corollary 7.3.** *The number  $N_1$  takes every value between  $q + 1 - \lfloor 2\sqrt{q} \rfloor$  and  $q + 1 + \lfloor 2\sqrt{q} \rfloor$  if and only if (a)  $q = p$  or (b)  $q = p^2$  with  $p = 2$  or  $p = 3$  or  $p \equiv 11 \pmod{12}$ .*

**Remark 7.4.** The only exceptional  $q < 1000$  is  $q = 128$ .

**Theorem 7.5.** *The number of points  $N_1$  on a non-singular cubic, for which the number  $n$  of rational inflexions is  $n = 0, 1, 3, 9$ , satisfies the following:*

(i) *If  $n = 0$ , then  $N_1 \equiv 0 \pmod{3}$ ;*

- (ii) If  $n = 1$ , then  $N_1 \equiv \pm 1 \pmod{3}$ ;
- (iii) If  $n = 3$ , then  $N_1 \equiv 0 \pmod{3}$ ;
- (iv) If  $n = 9$ , then  $N_1 \equiv 0 \pmod{9}$ .

Let  $A_q$  be the total number of isomorphism classes and  $P_q$  the total number of projective equivalence classes. Also,  $n_i$  for  $i = 0, 1, 3, 9$  is the number of projective equivalence classes with exactly  $i$  rational inflexions. Hence

$$A_q = n_9 + n_3 + n_1, \quad P_q = n_9 + n_3 + n_1 + n_0.$$

**Theorem 7.6.** (i)  $A_q = 2q + 3 + \left(\frac{-4}{q}\right) + 2\left(\frac{-3}{q}\right)$ ;

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

Here, the following Legendre–Jacobi symbols are used:

$$\left(\frac{-4}{c}\right) = \begin{cases} 1 & \text{if } c \equiv 1 \pmod{4}, \\ 0 & \text{if } c \equiv 0 \pmod{2}, \\ -1 & \text{if } c \equiv -1 \pmod{4}; \end{cases}$$

$$\left(\frac{-3}{c}\right) = \begin{cases} 1 & \text{if } c \equiv 1 \pmod{3}, \\ 0 & \text{if } c \equiv 0 \pmod{3}, \\ -1 & \text{if } c \equiv -1 \pmod{3}. \end{cases}$$

The number of inequivalent types of cubic with a fixed number of rational points can also be given. Let  $A_q(t)$  and  $P_q(t)$  be the number of inequivalent non-singular cubics with exactly  $q + 1 - t$  rational points under isomorphism and projective equivalence. So

$$A_q = \sum_t A_q(t), \quad P_q = \sum_t P_q(t).$$

The values of  $A_q(t)$  and  $P_q(t)$ , due to Schoof [9], are also given in [5, Section 11.11].

## 8 Some new applications in finite geometries

Much of finite geometries is concerned with maximal sets of points in  $\text{PG}(2, q)$  obeying various geometrical conditions: such sets are often of considerable interest also in algebraic coding theory. For example, a key result in the theory of MDS codes has as its foundation a famous theorem of the late B. Segre. This result asserts that, for  $q$  odd, a set of points with no 3 collinear has size at most  $q + 1$  with equality if and only if the set is the point set of a non-degenerate conic.

The next result, found independently by A. Zirilli and P.M. Neumann, see [2], is usually phrased using elliptic curves, that is, non-singular cubic curves with an inflexion point. However, as is seen below, this assumption is not necessary.

Table 3: Number of inequivalent cubics

$q \equiv m \pmod{12}$ $m$	$n_9$	$n_3$	$n_1$	$n_0$	$A_q$	$P_q$
3	0	$q - 1$	$q + 3$	$q - 1$	$2q + 2$	$3q + 1$
9	0	$q - 1$	$q + 5$	$q - 1$	$2q + 4$	$3q + 3$
2, 8	0	$q - 1$	$q + 2$	$q - 1$	$2q + 1$	$3q$
4	$\frac{1}{12}(q + 8)$	$\frac{1}{3}(2q + 4)$	$\frac{1}{4}(5q + 12)$	$q + 1$	$2q + 5$	$3q + 6$
1	$\frac{1}{12}(q + 11)$	$\frac{1}{3}(2q + 4)$	$\frac{1}{4}(5q + 15)$	$q + 1$	$2q + 6$	$3q + 7$
7	$\frac{1}{12}(q + 5)$	$\frac{1}{3}(2q + 4)$	$\frac{1}{4}(5q + 9)$	$q + 1$	$2q + 4$	$3q + 5$
5	0	$q - 1$	$q + 3$	$q - 1$	$2q + 2$	$3q + 1$
11	0	$q - 1$	$q + 1$	$q - 1$	$2q$	$3q - 1$

**Theorem 8.1.** *If a non-singular cubic curve  $\mathcal{C}$  has an even number  $k$  of rational points, then there exists a set  $\mathcal{S}$  of  $k/2$  points of  $\mathcal{C}$  with no three collinear.*

**Proof** Let  $G$  be the abelian group obtained from  $\mathcal{C}$ , using the general construction of Section 4 and the notation there. Then, from Theorem 4.1, three points on  $\mathcal{C}$  are collinear if and only if they add up to  $N$ . Let  $H$  be the subgroup of index 2 in  $G$ . There is another coset  $K$  of  $H$  in  $G$  so that  $G$  is the disjoint union of  $H$  and  $K$ . There are two cases:

- (i)  $N$  lies in  $H$ ;
- (ii)  $N$  lies in  $K$ .

In case (i), take  $\mathcal{S}$  to be the set  $K$ . Suppose that  $P, Q, R$  are in  $K$ . Then  $P \oplus Q$  must be in  $H$  so that  $P \oplus Q \oplus R$  must be in  $K$ . In particular,  $P \oplus Q \oplus R$  cannot be equal to  $N$ , which is in  $H$ . Therefore  $\mathcal{S}$  is a set of  $k/2$  points with no 3 collinear.

In case (ii), take  $\mathcal{S}$  to be the set  $H$ . Let  $P, Q, R$  be any 3 points of  $\mathcal{S}$ . Since  $H$  is a subgroup,  $P \oplus Q \oplus R$  is in  $H$ . In particular,  $P \oplus Q \oplus R$  cannot equal  $N$  since  $N$  is in  $K$ . Thus  $\mathcal{S}$  is a set of  $k/2$  points, with no 3 collinear.  $\square$

**Remark 8.2.** It is possible that such sets  $\mathcal{S}$  are not maximal when considered as sets of points in  $\text{PG}(2, q)$  with no 3 collinear.

So far, sets of points with no three collinear have been considered. As any two points define a unique line, the next step is to try to find a result analogous to Theorem 8.1 for higher degree curves.

Theorem 8.1 can be generalised as follows.

**Theorem 8.3.** *Let  $\mathcal{C}$  be a non-singular cubic curve in  $\text{PG}(2, q)$  containing exactly  $n$  points and with a cyclic group structure. Suppose the integer  $r$  divides  $n$ . Then there exists a set  $\mathcal{S}$  of  $n/r$  points on  $\mathcal{C}$  satisfying the following condition: no  $3k$  points of  $\mathcal{S}$  lie on any curve of degree  $k$  other than  $\mathcal{C}$  whenever  $1 \leq k < \lceil r/3 \rceil$ .*

**Proof** The group  $G$  has a subgroup  $H$  of order  $n/r$  and index  $r$ . The cosets of  $H$  are denoted by  $H = H_0, H_1, H_2, \dots, H_{r-1}$ , where  $H_i \oplus H_j = H_{i+j \pmod{r}}$ .

Let  $H_j$  be the coset containing the point  $N$ . Take  $\mathcal{S} = H_i$  where  $i$  is to be determined. Choose any  $3k$  points  $P_1, P_2, \dots, P_{3k}$  in  $\mathcal{S}$ . Their sum lies in the coset  $3kH_1 = H_{3k \pmod{r}}$ . Using Theorem 4.2,  $\mathcal{S}$  has the desired property if the sum of these  $3k$  points is always different from  $kN$ . This will follow from showing that the cosets  $H_{3ki \pmod{r}}$  and  $H_{kj \pmod{r}}$  are unequal; that is  $k(3i - j) \not\equiv 0 \pmod{r}$ .

There are three cases to consider:

- (i) 3 does not divide  $r$ ;
- (ii) 3 divides  $r$  but 3 does not divide  $j$ ;
- (iii) 3 divides both  $r$  and  $j$ .

In case (i), 3 does not divide  $r$ . Then 3 has a multiplicative inverse  $u$  modulo  $r$ . Put  $i = uj + u$ . Then  $3i - j \equiv 1 \pmod{r}$ . Thus, if  $k(3i - j) \equiv 0 \pmod{r}$ , then  $k \equiv 0 \pmod{r}$ . The hypotheses imply that  $0 < k < r$ . So  $\mathcal{S} = H_i$  has the desired property.

In case (ii), if  $j \equiv 2 \pmod{3}$  then put  $i = (j + 1)/3$ . If  $j \equiv 1 \pmod{3}$  then put  $i = (j - 1)/3$ . Thus  $3i - j$  is either 1 or  $-1$  modulo  $r$ . Hence, if  $k(3i - j) \equiv 0 \pmod{r}$ , then  $k \equiv 0 \pmod{r}$ . As in case (i), this implies that  $\mathcal{S}$  has the required property.

In case (iii), put  $i = j/3 + 1$ . Then  $3i - j = 3$ . If  $k(3i - j) \equiv 0 \pmod{r}$  then  $3k \equiv 0 \pmod{r}$ . But this contradicts the assumed bounds on  $k$ . Again this implies that  $\mathcal{S}$  has the desired property.  $\square$

**Remark 8.4.** In this proof, only the fact that  $G/H$  is cyclic is used. Strictly speaking, the assumption that  $G$  is cyclic can be weakened to merely assuming that  $G/H$  is cyclic.

**Remark 8.5.** In the statement of the theorem, the restriction that  $k < \lceil r/3 \rceil$  is only required in case (iii). In the other two cases, it is sufficient to assume that  $k < r$ .

**Remark 8.6.** Concerning the sets constructed in Theorem 8.1, Voloch [12] has shown that, in many cases, they cannot be extended to larger sets with no 3 points collinear. In [1], it is shown that these results of Voloch can be strengthened and generalised.

The research of the first author is supported by grants from NSERC. The research of the third author is supported by grants from ARP and NSERC.

## References

- [1] T.L. Alderson, A.A. Bruen, and R. Silverman, Maximum distance separable codes and arcs in projective spaces, *J. Combin. Theory Ser. A* **114** (2007), 1101–1117.
- [2] A.A. Bruen, Arcs and multiple blocking sets, *Combinatorica*, Symposia Mathematica **28**, 1984, 15–29.
- [3] A.A. Bruen and M.A. Forcinito, *Cryptography, Information Theory, and Error-Correction*, Wiley, Hoboken, 2005, xxiii+468 pp.
- [4] W. Fulton, *Algebraic Curves*, Benjamin, New York, 1969, xiii+226 pp.
- [5] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Second edition, Oxford Mathematical Monographs, Oxford University Press, Oxford, 1998, xiv+555 pp.
- [6] J.W.P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic Curves over a Finite Field*, Princeton University Press, Princeton, 2008, xxii+696 pp.
- [7] F. Lang, Geometry and group structures of some cubics, *Forum Geom.* **2** (2002), 135–146 (electronic).
- [8] H. Rück, A note on elliptic curves over a finite field, *Math. Comp.* **49** (1987), 201–304.
- [9] R. Schoof, Nonsingular plane cubic curves over finite fields, *J. Combin Theory Ser. A* **46** (1987), 183–211.
- [10] J.H. Silverman, The arithmetic of elliptic curves. Corrected reprint of the 1986 original. Graduate Texts in Mathematics **106**, Springer Verlag, New York, 1992, xii+400 pp.
- [11] M. Tallini Scafati, Graphic curves on a Galois plane, *Atti del Convegno di Geometria Combinatoria e sue Applicazione*, Università di Perugia, Perugia, 1971, 413–419.
- [12] J.F. Voloch, On the completeness of certain plane arcs, *European J. Combin.* **8** (1987), 453–456.
- [13] J.F. Voloch, A note on elliptic curves over finite fields, *Bull. Soc. Math. France* **116** (1988), 455–458.
- [14] W.C. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. École Normale Sup.* **4** (1969), 521–560.



A.A. Bruen  
Department of Electrical  
and Computer Engineering  
University of Calgary  
Calgary  
Alberta T2N 1N4  
Canada  
bruen@ucalgary.ca

J.W.P. Hirschfeld  
Department of  
Mathematics  
University of Sussex  
Brighton  
East Sussex BN1 9RF  
United Kingdom  
jwph@sussex.ac.uk

D.L. Wehlau  
Department of Mathematics  
and Computer Science  
Royal Military College  
Kingston  
Ontario K7K 7B4  
Canada  
wehlau@rmc.ca