Rendiconti di Matematica, Serie VII
Volume 30, Roma (2010), 77-88

Curves of genus 3

J.W.P. HIRSCHFELD

Dedicated to Marialuisa de Resmini on her retirement

Abstract: *Any curve of genus 3 can be represented as a plane quartic curve. The question of the maximum number of points on such a curve over a finite field is discussed.*

1 – Questions about curves

(i) What is meant by the 'number of points' on a curve?
(ii) What is the number of points on a curve that can occur, given some parameters such as
q, the size of the field,
g, the genus of the curve,
n, the degree of a plane curve?
(iii) What is the maximum number of points?
(iv) Find curves with certain parameters.
(v) Classify the curves with a set of these parameters.

One such problem is to find the number of rational points over $\mathbf{F}_q$ on a non-singular plane quartic curve, that is, a curve of genus 3.

This article surveys this problem and its background. For contrast, curves of genus 1 and 2 are also considered.

Key Words and Phrases: *Cubic surface – Quartic curve*
A.M.S. Classification: 11G25, 51E20.

2 – Cubic surfaces

Let $\mathcal{V} = \mathbf{v}(F_1, \ldots, F_r)$ be the variety given by the zeros of the homogeneous polynomials $F_1, \ldots, F_r$.

THEOREM 2.1. *A non-singular surface $\mathcal{F}^3$ of degree three over a field K has at most 27 lines and over the algebraic closure $\overline{K}$ exactly 27 lines.*

THEOREM 2.2. *Over $\mathbf{F}_q$, there exists an $\mathcal{F}^3$ with 27 lines if $q \neq 2, 3, 5$. Equivalently, in $\mathrm{PG}(2, \mathrm{q})$, there exists a 6-arc not on a conic if $q \neq 2, 3, 5$.*

THEOREM 2.3.
(i) *The group G_{27} of automorphisms of the 27 lines is isomorphic to*

$$\mathrm{P\Gamma U}(4,4) \cong \mathrm{PGO}_-(6,2) \cong \mathrm{PGSp}(4,3) \cong \mathrm{PGO}(5,3),$$

and has order $51,840 = 72 \times 6!$.
(ii) *The simple group G'_{27} of index two in G_{27} is isomorphic to $\mathrm{PGU}(4,4)$, and has order $25,920 = 36 \times 6!$.*

2.1 – From 27 to 28

THEOREM 2.4. *For a point P not on a line of $\mathcal{F}^3$, the intersection $\mathcal{C}^6$ of $\mathcal{F}^3$ and the polar quadric $\mathcal{Q}^2$ of $\mathcal{F}^3$ at P has a double point at P; it projects from P to a non-singular plane quartic when K has characteristic other than two.*

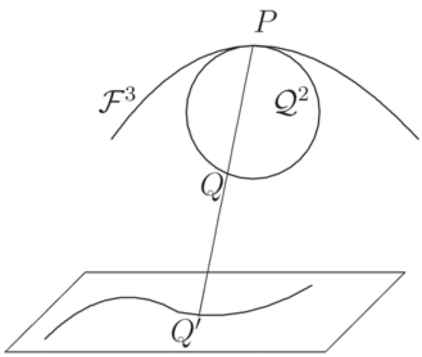


Figure 1
$\mathcal{F}^3 \cap \mathcal{Q}^2 = \mathcal{C}^6 \xrightarrow{P} \mathcal{C}^4$

Proof. Let $P = (1,0,0,0)$ and $\pi = \mathbf{v}(X_0)$. Then

$$\begin{aligned}\mathcal{F}^3 &= \mathbf{v}(X_0^2 f_1(X_1,X_2,X_3) + X_0 f_2(X_1,X_2,X_3) + f_3(X_1,X_2,X_3)),\\ \mathcal{Q}^2 &= \mathbf{v}(2X_0 f_1(X_1,X_2,X_3) + f_1(X_1,X_2,X_3)),\\ \mathcal{C}^6 &= \mathbf{v}(X_0^2 f_1 + X_0 f_2 + f_3,\ 2X_0 f_1 + f_2)\\ \mathcal{C}^4 &= \mathbf{v}(f_2^2 - 4 f_1 f_3, X_0)\end{aligned}$$

For q even, $\mathcal{C}^4 = \mathcal{C}^2 \cup \mathcal{C}^2$, a repeated conic. For q odd, $\mathcal{F}^3$ is non-singular if and only if $\mathcal{C}^4$ is non-singular. □

Theorem 2.5. *For q odd, $q \geq 9$, there exists a non-singular $\mathcal{C}^4$ with 28 bitangents if and only if there exists $\mathcal{F}^3$ with 27 lines and P not on the lines.*

Example 2.6. For $q = 9$, let

$$\begin{aligned}F &= X_0^4 + X_1^4 + X_2^4\\ &= X_0\bar{X}_0 + X_1\bar{X}_1 + X_2\bar{X}_2,\end{aligned}$$

where $t \mapsto t^3 = \bar{t}$ is the involutory automorphism of $\mathbf{F_9}$. So $\mathcal{F} = \mathbf{v}(F)$ is a Hermitian curve with $q\sqrt{q}+1 = 28$ rational points, all of which are undulations; that is, the tangents have 4-point contact and so are bitangents.

2.2 – Number of points

Theorem 2.7.

(i) *The number of rational points on a non-singular cubic surface $\mathcal{F}^3$ over $\mathbf{F}_q$ is $|\mathcal{F}^3(\mathbf{F}_q)| = q^2 + 7q + 1$.*

(ii)
- (a) *The 27 lines of $\mathcal{F}^3$ lie on 45 tritangent planes of which e meet $\mathcal{F}^3$ in three concurrent lines.*
- (b) *The number of rational points on the lines is $N_0 = 27(q-4) + e$.*

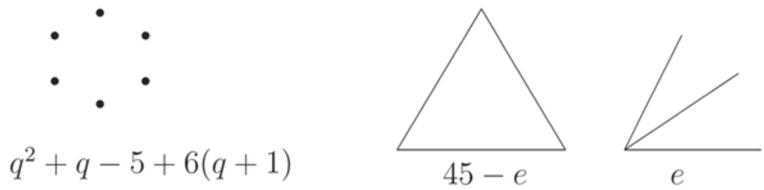
Proof.

(i) In the correspondence between $\mathcal{F}^3$ and the plane, each line in one half of a double-six corresponds to a point.

(ii) (b) A triangle contains $3q$ points, whereas a triad of concurrent lines contains $3q+1$ points. As each line meets 10 others, a count of points on just one of the 27 lines plus those on more than one line gives the following:

$$N_0 = 27(q + 1 - 10) + 27 \times 10/2 + e.$$

□



2.3 – Full $\mathcal{F}^3$

Definition 2.8. A cubic surface defined over K is *full* if its lines contain all its rational points.

Theorem 2.8.

(i) *There exists a full* $\mathcal{F}^3$ *for*

$$q = 4,\ 7,\ 8,\ 9,\ 11,\ 13,\ 16\,.$$

(ii) *Canonical forms for the full surfaces are as follows*:

$$\begin{aligned}
\mathcal{E} &= \mathbf{v}(X_0^3 + X_1^3 + X_2^3 + X_3^3), \quad q = 4, 7, 13, 16;\\
\mathcal{D} &= \mathbf{v}\left(X_0^3 + X_1^3 + X_2^3 + X_3^3 + X_4^3, \sum X_i\right), \quad q = 4, 11, 16;\\
\mathcal{D} &= \mathbf{v}\left(\sum X_i X_j X_k, \sum X_i\right), \quad q = 9;\\
\mathcal{C} &= \mathbf{v}(X_0X_1(X_0 + X_1) + X_2X_3(X_0 + X_2 + X_3)), \quad q = 8.
\end{aligned}$$

(iii) *For* $q = 4, 7, 8$, *every* $\mathcal{F}^3$ *is full.*

(iv) *For* $q > 16$, *no* $\mathcal{F}^3$ *is full.*

2.4 – Number of lines and bitangents

Theorem 2.10. *For a cubic surface* $\mathcal{F}_3$ *and the corresponding* $\mathcal{C}_4$ *over* $\mathbf{F}_q$, *let* n *be the number of possible lines on* $\mathcal{F}_3$ *and* b *the number of possible bitangents on* $\mathcal{C}_4$.

(i) *For* q *odd*,

$$n = 27,\ 15,\ 9,\ 7,\ 5,\ 3,\ 2,\ 1,\ 0;$$
$$b = 28,\ 16,\ 10,\ 8,\ 6,\ 4,\ 3,\ 2,\ 1,\ 0.$$

(ii) *For* $q = 2$,

$$n = 15,\ 9,\ 5,\ 3,\ 2,\ 1,\ 0.$$

QUESTION 2.11. What are the possible numbers of lines on a non-singular cubic over $\mathbf{F}_{\mathbf{2^h}}$?

THEOREM 2.12. *For q even, the possible numbers of bitangents of a non-singular plane quartic are* 7, 3, 1, 0. *In the case of* 7 *bitangents they form a* PG(2, 2).

EXAMPLE 2.13. (The Klein curve for $q = 8$)

$$\mathcal{F} = \mathbf{v}(X^3Y + Y^3Z + Z^3X).$$

The 24 rational points are all inflexions. There are 7 bitangents

$$\mathbf{v}(c^3X + cY + Z), \quad c \in \mathbf{F_8}\backslash\{\mathbf{0}\},$$

forming a PG(2, 2).

THEOREM 2.14. *For an algebraically closed field of characteristic two, the possible configurations of bitangents are the following* :

(1) 7 *lines forming a* PG(2, 2);
(2) 4 *lines with* 3 *concurrent*;
(3) 1 *line*;
(4) *a pencil plus a line*;
(5) *a pencil with one special line.*

3 – The number of points on a non-singular curve

For a curve $\mathcal{F}$ defined over $\mathbf{F}_q$ with N_i the number of points of $\mathcal{F}$ rational over $\mathbf{F}_{\mathbf{q^i}}$, the *zeta function* is

$$\zeta_q(T) = \exp(1 + N_1T + N_2T^2/2 + N_3T^3/3 + \cdots).$$

THEOREM 3.1. (*Hasse–Weil*)

$$\zeta_q(T) = \exp\left(\sum N_iT^i/i\right) = \frac{f(T)}{(1-T)(1-qT)},$$

with $f \in \mathbf{Z}[T], \quad \deg f = 2g.$

Corollary 3.2.
(i) $N_1 \leq q + 1 + 2g\sqrt{q}$.
(ii) *When* $g = 1$,

$$\zeta_q(T) = \frac{1 + c_1 T + qT^2}{(1-T)(1-qT)}.$$

Theorem 3.3. (*Serre*) $N_1 \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor$.

Notation 3.4. $N_q(g) = \max N_1$, taken over all non-singular curves $\mathcal{C}$ of genus g over $\mathbf{F}_q$.

Example 3.5. For the Klein curve with $q = 2$,

$$\begin{aligned}
&F = X^3Y + Y^3Z + Z^3X, \\
&N_1 = 3, \quad N_2 - N_1 = 2, \quad N_3 - N_1 = 21, \\
&f(T) = 1 + 5T^3 + 8T^6.
\end{aligned}$$

A special case of an important theorem gives other bounds.

Theorem 3.6. (*Stöhr–Voloch*) *For a plane curve of degree* n *with not all points inflexions and* $p \neq 2$,

$$N_1 \leq \frac{1}{2} n(n + q - 1).$$

The case that $q = 7, n = 4, g = 3$ gives

$$N_7(3) \leq 20 < 23 = 7 + 1 + 3\lfloor 2 \times \sqrt{7} \rfloor$$

In fact, $N_7(3) = 20$.

4 – Curves of genus 1

A curve of genus 1, or elliptic curve, can be regarded as a plane non-singular cubic. Plane cubics may be classified up to isomorphism or projective equivalence.

Theorem 4.1. *Up to isomorphism, a curve* $\mathcal{F} = \mathbf{v}(F)$ *of genus* 1 *over* $\mathbf{F}_q$, *with* $q = p^h$, *has at least one point of inflexion and the following canonical forms.*

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

$$F \;=\; Y^2Z + X^3 + cXZ^2 + dZ^3,$$

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

(ii) *When* $p = 3$,

(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) *When* $p = 2$,

(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* $(q-1,3) = 1$ *and* $e = 1, \alpha, \alpha^2$ *when* $(q-1,3) = 1$, *with* α *a primitive element of* $\mathbf{F}_q$*; also,* $d = 0$ *or a particular element of trace* 1.

Canonical forms up to a projectivity exist for cubics with no inflexions; see [7, Chapter 11]. For example, over $\mathbf{F_7}$, let

$$F = X^3 + 2Y^3 + 3Z^3.$$

The corresponding curve $\mathcal{F}$ has no inflexion.

THEOREM 4.2. *Let* N_1 *be the number of rational points of an elliptic curve over* $\mathbf{F}_q$.

(i)

$$q + 1 - 2\sqrt{q} \leq N_1 \;\leq\; q + 1 + 2\sqrt{q}.$$

(ii) *The precise number* $N_1 = q + 1 - t$, *with* $|\,t\,| \leq 2\sqrt{q}$, *of points that can occur is given in Table 1.*

TABLE 1: VALUES OF t

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

THEOREM 4.3. *If A_q and P_q are the numbers of distinct elliptic curves up to isomorphism and projective equivalence, then*

$$A_q = 2q + 3 + \left(\frac{-4}{q}\right) + 2\left(\frac{-3}{q}\right);$$

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

Here the bracketed numbers are Legendre and Legendre–Jacobi symbols taking the values $-1, 0, 1$.

The prime power $q = p^h$ is *exceptional* if h is odd, $h \geq 3$, and p divides $\lfloor 2\sqrt{q} \rfloor$.

THEOREM 4.4. *The actual upper bounds for elliptic curves over $\mathbf{F}_q$ are as follows:*

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

COROLLARY 4.5. *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) $q = p$;
(b) $q = p^2$ *with* $p = 2$ *or* $p = 3$ *or* $p \equiv 11 \pmod{12}$.

4.1 – Unsolved problem

Let $m_3(2,q)$ be the maximum size of a point set $\mathcal{K}$ in $\mathrm{PG}(2,q)$ such that at most three points of $\mathcal{K}$ lie on a line. Show that

$$m_3(2,q) > N_q(1) \quad \text{for } q \neq 4.$$

This is true for $q \leq 13$ as in Table 2.

TABLE 2: VALUES OF $m_3(2,q)$

q	2	3	4	5	7	8	9	11	13
$m_3(2,q)$	7	9	9	11	15	15	17	21	23
$N_q(1)$	5	7	9	10	13	14	16	18	21

5 – Curves of genus 2

THEOREM 5.1. *For a curve of genus* 2 *over* $\mathbf{F}_q$ *with* q *square,*

$$\begin{aligned} &N_q(2) = q + 1 + 4\sqrt{q}, \quad \text{if } q \neq 4, 9;\\ &N_4(2) = 10;\\ &N_9(2) = 20. \end{aligned}$$

The prime power $q = p^h$ is *special* if (a) or (b) holds:

(a) p divides $\lfloor 2\sqrt{q} \rfloor$;
(b) there exists m such that $q = m^2 + 1$ or $q = m^2 + m + 1$ or $q = m^2 + m + 2$.

THEOREM 5.2. *If* q *is a non-square, with* $\{2\sqrt{q}\} = 2\sqrt{q} - \lfloor 2\sqrt{q} \rfloor$,

$$\begin{aligned} N_q(2) &= q + 1 + 2\lfloor 2\sqrt{q} \rfloor, && \text{if } q \text{ is not special};\\ N_q(2) &= q + 2\lfloor 2\sqrt{q} \rfloor, && \text{if } q \text{ is special and } \{2\sqrt{q}\} > \tfrac{1}{2}(\sqrt{5} - 1);\\ N_q(2) &= q - 1 + 2\lfloor 2\sqrt{q} \rfloor, && \text{if } q \text{ is special and } \{2\sqrt{q}\} < \tfrac{1}{2}(\sqrt{5} - 1). \end{aligned}$$

6 – Curves of genus 3

From Section 3, there is the following result.

THEOREM 6.1.
(i) $N_q(3) \leq q + 1 + 3\lfloor 2\sqrt{q} \rfloor = S_3$.

(ii) $$N_q(3) \leq \begin{cases} 28, & q = 9 \\ 2(q+3), & q \text{ odd, } q \neq 9 \\ 2(q+4), & q \text{ even} \end{cases} = V_3.$$

THEOREM 6.2. (*Lauter*) *For a curve of genus* 3,

$$\left.\begin{array}{ll} N_1 \leq q - 1 + 3\lfloor 2\sqrt{q} \rfloor & \text{if } q = m^2 + 1; \\ N_1 \leq q - 1 + 3\lfloor 2\sqrt{q} \rfloor & \text{if } q = m^2 + 2 \text{ with } m \geq 2; \\ N_1 \leq q - 2 + 3\lfloor 2\sqrt{q} \rfloor & \text{if } q = m^2 + m + 1; \\ N_1 \leq q - 2 + 3\lfloor 2\sqrt{q} \rfloor & \text{if } q = m^2 + m + 3 \text{ with } m \geq 3. \end{array}\right\} = L_3$$

THEOREM 6.3. *For a curve of genus* 3, *if* $N_1 > 2q + 6$ *then one of the following holds*:

(i) $N_1 = 28$, $q = 9$ *and* $\mathcal{C}$ *is the Hermitian curve*;
(ii) $N_1 = 24$, $q = 8$ *and* $\mathcal{C}$ *is the Klein curve.*

Table 3 summarises the results for small q.

TABLE 3: NUMBER OF POINTS ON CURVES OF GENUS 3

q	2	3	4	5	7	8	9	11	13	16	17	19	23	25	27
$N_q(3)$	7	10	14	16	20	24	28	28	32	38	40	44	48	56	56
S_3	9	13	17	18	23	24	28	30	35	41	42	44	51	56	58
V_3	10	12	16	16	20	24	28	28	32	40	40	44	52	56	60
L_3	7	10		16	20			28	32		40		48		56

THEOREM 6.4. (*Ibukiyama*) *For* $q = p^{4m+2}$,

$$N_q(3) = q + 1 + 6\sqrt{q}.$$

THEOREM 6.5.

(i) *When $q < 100$, there is equality $N_q(3) = S_3$ if and only if*

$$q \in \{8, 9, 19, 25, 29, 41, 47, 49, 53, 61, 64, 67, 71, 79, 81, 89, 97\}.$$

(ii) *When $q \leq 27$, there is equality $N_q(3) = V_3$ if and only if*

$$q \in \{5, 7, 11, 13, 17, 19, 25\}.$$

REFERENCES

[1] A. D. CAMPBELL: *Plane quartic curves in the Galois fields of order* 2^n, Tôhoku Math. J. **37** (1933) pp. 88–93.

[2] L. R. A. CASSE: *Concerning bitangents of irreducible plane quartic curves over* $GF(2^h)$, Teorie Combinatorie, vol. II, Accad. Naz. dei Lincei, Rome, 1976, (Rome, 1973), pp. 381–387.

[3] M. J. DE RESMINI: *Sulle quartiche piane sopra un campo di caratteristica due*, Ricerche Mat. **19** (1970) pp. 133–160.

[4] L. E. DICKSON: *Classification of quartic curves*, modulo 2, Messenger of Mathematics, **44** (1915), pp. 189–192.

[5] L. E. DICKSON: *Geometrical and invariantive theory of quartic curves*, modulo 2, Amer. J. Math., **37** (1915) pp. 337–354.

[6] L. E. DICKSON: *Quartic curves*, modulo 2, Trans. Amer. Math. Soc., **16** (1915) pp. 111–120.

[7] J. W. P. HIRSCHFELD: *Projective Geometries over Finite Fields*, second edition, Oxford University Press, Oxford, 1998, xiv p. 555.

[8] J. W. P. HIRSCHFELD: *Finite Projective Spaces of Three Dimensions*, Oxford University Press, Oxford, 1985, x p. 316.

[9] J. W. P. HIRSCHFELD – G. KORCHMÁROS – F. TORRES: *Algebraic Curves over a Finite Field*, Princeton University Press, Princeton, 2008, xxii p. 696.

[10] T. IBUKIYAMA: *On rational points of curves of genus 3 over finite fields*, Tohoku Math. J., **45** pp. 311–329.

[11] R. H. JEURISSEN – C. H. VAN OS – J. H. STEENBRINK: *The configuration of the bitangents of the Klein curve*, Discrete Math., **132** (1994) pp. 83–96.

[12] K. LAUTER: *The maximum or minimum number of rational points on genus three curves over finite fields*, Compositio Math., **134** (2002) pp. 87–111 (Appendix by J.-P. Serre).

[13] B. SEGRE: *Arithmetical Questions on Algebraic Varieties*, The Athlone Press, University of London, London, 1951, p. 55

[14] J. Top: *Curves of genus 3 over small finite fields*, Indag. Math., **14** pp. 275–283.

Lavoro pervenuto alla redazione il 10 marzo 2010
ed accettato per la pubblicazione il 15 marzo 2010.
Bozze licenziate il 20 aprile 2010

Indirizzo dell'Autore:

J. W. P. Hirschfeld – Department of Mathematics – University of Sussex – Brighton BN1 9RF
United Kingdom
Email: jwph@sussex.ac.uk – http://www.maths.sussex.ac.uk/Staff/JWPH/