MATHEMATICS OF COMPUTATION
VOLUME 49, NUMBER 179
JULY 1987, PAGES 301-304

A Note on Elliptic Curves Over Finite Fields

By Hans-Georg Rück

Abstract. Let E be an elliptic curve over a finite field k and let $E(k)$ be the group of k-rational points on E. We evaluate all the possible groups $E(k)$ where E runs through all the elliptic curves over a given fixed finite field k.

Let k be a finite field with $q = p^n$ elements. An elliptic curve E over k is a projective nonsingular curve given by an equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1}$$

with coefficients $a_1, \ldots, a_6$ in k. For each field $\tilde{k}$ that contains k, the set $E(\tilde{k})$ of points with coordinates in $\tilde{k}$ satisfying (1) forms an Abelian group whose zero element can be chosen as the element $(0,1,0)$. In this note we want to look at the following Question 1: Given a fixed finite field k, what are the possible Abelian groups $E(k)$, when the coefficients of the equation (1) vary over all the possible values in k? The answer to this question is given in Theorem 3. If we just look at the possible orders $\#E(k)$, the appropriate Question 2 was answered by Waterhouse [4] (see also Deuring [1] for $k = \mathbf{F}_p$) using the theorem of Honda and Tate [3] for Abelian varieties over finite fields.

THEOREM 1a [4]. *All the possible orders* $h = \#E(k)$ are given by $h = 1 + q - \beta$, where β is an integer with $|\beta| \leqslant 2\sqrt{q}$ satisfying one of the following conditions*:
(a) $(\beta, p) = 1$;
(b) *If n is even*: $\beta = \pm 2\sqrt{q}$;
(c) *If n is even and $p \not\equiv 1$* mod 3: $\beta = \pm\sqrt{q}$;
(d) *If n is odd and $p = 2$ or* 3: $\beta = \pm p^{(n+1)/2}$;
(e) *If either* (i) *n is odd or* (ii) *n is even, and $p \not\equiv 1$* mod 4: $\beta = 0$.

Following the general ideas of Waterhouse [4] we can also give an answer to the first question.

For an elliptic curve E over k let $\mathrm{End}(E)$ be the ring of group endomorphisms of E which are given by algebraic equations with coefficients in k. It is known that $\mathrm{End}(E)$ is an order in a finite-dimensional division algebra over $\mathbf{Q}$. This division algebra determines $\#E(k)$:

THEOREM 2 [2]. *Let E, E' be elliptic curves over k; then*

$$\#E(k) = \#E'(k) \quad \textit{if and only if} \quad \mathrm{End}(E) \otimes_{\mathbf{Z}} \mathbf{Q} = \mathrm{End}(E') \otimes_{\mathbf{Z}} \mathbf{Q}.$$

Received July 9, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11G20.

*Here "possible orders" or "possible groups" mean that these orders or groups really occur.

There is a special endomorphism π, called the Frobenius endomorphism, which maps a point $P = (x, y, z)$ on E to $\pi(P) = (x^q, y^q, z^q)$ on E. From this definition it follows immediately that $E(k)$ is the set of all the points P on E with $\pi(P) = P$.

If h is a fixed possible order $\#E(k)$, then by Theorem 2 the division algebra $K = \operatorname{End}(E) \otimes_{\mathbf{Z}} \mathbf{Q}$ is fixed. What are the orders in K that are rings of endomorphisms of elliptic curves over k? The answer is:

THEOREM 1b [4]. *Let $h = 1 + q - \beta$ be a possible order $\#E(k)$, where β satisfies one of the conditions* (a), ..., (e) *of Theorem* 1a.

In case (a): *$K = \mathbf{Q}(\pi)$ is an imaginary quadratic field over $\mathbf{Q}$; all the orders in K are possible endomorphism rings.*

In case (b): *K is a division algebra of order* 4 *with center $\mathbf{Q}$, π is a rational integer, all the maximal orders in K are possible endomorphism rings.*

In cases (c), (d), (e): *$K = \mathbf{Q}(\pi)$ is an imaginary quadratic field over $\mathbf{Q}$, all the orders in K whose conductor is prime to p are possible endomorphism rings.*

Let h be a possible order and $h = \prod_l l^{h_l}$ its decomposition in powers of prime numbers. Since the genus of an elliptic function field is one, the possible $E(k)$ with $\#E(k) = h$ are among all the groups of the form

$$\mathbf{Z}/p^{h_p}\mathbf{Z} \times \prod_{l \neq p} \left(\mathbf{Z}/l^{a_l}\mathbf{Z} \times \mathbf{Z}/l^{h_l - a_l}\mathbf{Z}\right) \quad \text{with } 0 \leqslant a_l \leqslant h_l.$$

The relation between $\operatorname{End}(E)$ and the structure of $E(k)$ is given by the following lemma:

LEMMA 1. *Let m be a positive integer which is not divisible by p, and let E_m be the group of the points P on E with $mP = 0$. Then E_m is contained in $E(k)$ if and only if $\pi - 1$ is divisible by m in* $\operatorname{End}(E)$.

Proof. If $\pi - 1$ is divisible by m in $\operatorname{End}(E)$, then $\pi - 1 = \lambda \cdot m$ with $\lambda \in \operatorname{End}(E)$. Let $P \in E_m$, then $(\pi - 1)(P) = \lambda \cdot m(P) = 0$. Hence $\pi(P) = P$ and $E_m \subset E(k)$.

If $E_m \subset E(k)$, then the kernel of $\pi - 1$ contains the kernel of the multiplication by m. Since the multiplication by m is separable, the universal mapping property for Abelian varieties (see [5, p. 27, Proposition 10]) shows that $\pi - 1 = m \cdot \lambda$ with $\lambda \in \operatorname{End}(E)$.

LEMMA 2. *We assume that π is not contained in $\mathbf{Q}$; then by Theorem* 1b *the division algebra K is an imaginary quadratic field. The maximal order in K is denoted by O_K. Let l be a rational prime number which is different from p and suppose that $\pi - 1 = l^x \cdot \omega$, where $\omega \in O_K$ is not divisible by l. Then*

$$x = \min\left\{ v_l(q-1), \left[\frac{v_l(\#E(k))}{2}\right] \right\}. \tag{2}$$

([λ] *is the largest rational integer $\leqslant \lambda$; $v_l(\cdot)$ is the normalized valuation of $\mathbf{Z}$ corresponding to l.*)

Proof. The zeta function of E yields the equation

$$\#E(k) = (\pi - 1)(\bar{\pi} - 1) = q - (\pi + \bar{\pi}) + 1.$$

From this we get the two equations

$$\#E(k) = l^{2x} \cdot \omega \cdot \bar{\omega} \tag{3}$$

and

$$\#E(k) = (q-1) - (\pi - 1) - (\bar{\pi} - 1). \tag{4}$$

If l is prime to ω, then (3) yields $2x = v_l(\#E(k))$ and (4) yields

$$v_l(q-1) \geqslant \min\{x, v_l(\#E(k))\} \geqslant \left[\frac{v_l(\#E(k))}{2}\right].$$

This proves (2). If l is not prime to ω, then either l is decomposed or is ramified in O_K. Suppose $(l) = \mathscr{L} \cdot \bar{\mathscr{L}}$ in O_K with $\mathscr{L} \neq \bar{\mathscr{L}}$. Let, for example, $v_{\mathscr{L}}(\omega) > 0$. Then $v_{\bar{\mathscr{L}}}(\omega) = 0$ and $v_{\mathscr{L}}(\omega + \bar{\omega}) = 0$. Equation (3) yields $2x < v_l(\#E(k))$ and Eq. (4) yields $x \geqslant \min\{v_l(\#E(k)),\ v_l(q-1)\}$, where equality holds if $v_l(\#E(k))$ and $v_l(q-1)$ are different. A detailed examination of the possible values of $v_l(\#E(k))$ and $v_l(q-1)$ shows that (2) holds. Suppose $(l) = \mathscr{L}^2$ in O_K. If $v_{\mathscr{L}}(\omega) > 0$, then $v_{\mathscr{L}}(\omega) = 1$. Equation (3) yields $2x + 1 = v_l(\#E(k))$. Thus we get

$$x = \frac{v_l(\#E(k)) - 1}{2} = \left[\frac{v_l(\#E(k))}{2}\right].$$

Equation (4) shows that $v_l(q-1) \geqslant [v_l(\#E(k))/2]$, which proves (2).

We can now give an answer to the first question and prove the following theorem.

THEOREM 3. *Let k be a finite field with $q = p^n$ elements. Let $h = \prod_l l^{h_l}$ be a possible order $\#E(k)$ of an elliptic curve E over k. Then all the possible groups $E(k)$ with $\#E(k) = h$ are the following*:

$$\mathbf{Z}/p^{h_p}\mathbf{Z} \times \prod_{l \neq p} \left(\mathbf{Z}/l^{a_l}\mathbf{Z} \times \mathbf{Z}/l^{h_l - a_l}\mathbf{Z}\right)$$

with

(a) *In case* (b) *of Theorem* 1a: *Each a_l is equal to $h_l/2$*;

(b) *In cases* (a), (c), (d), (e) *of Theorem* 1a: *a_l is an arbitrary integer satisfying* $0 \leqslant a_l \leqslant \min\{v_l(q-1), [h_l/2]\}$.

Proof. (a) In case (b) of Theorem 1a we get $\pi \in \mathbf{Z}$ and $h = (\pi - 1)^2$. Furthermore, $\pi - 1$ is divisible by m in $\mathrm{End}(E)$ if and only if $\pi - 1$ is divisible by m in $\mathbf{Z}$. Hence Lemma 1 shows that $a_l = \min\{v_l(\pi - 1), [h_l/2]\} = h_l/2$.

(b) Let $\{1, \eta\}$ be an integral basis of O_K. Then $\pi = a + b\eta$ with $a, b \in \mathbf{Z}$ and $b \neq 0$. This yields $\pi - 1 = a - 1 + b\eta$ with

$$\min\{v_l(a-1),\ v_l(b)\} = \min\{v_l(q-1),\ [h_l/2]\}$$

by Lemma 2. For each $l \neq p$ let a_l be arbitrary with

$$0 \leqslant a_l \leqslant \min\{v_l(q-1), [h_l/2]\}.$$

Consider the order R in O_K whose conductor is equal to $\prod_{l \neq p} l^{v_l(b) - a_l}$. There is an elliptic curve E over k with $R = \mathrm{End}(E)$ by Theorem 1b. The exact l-power that divides $\pi - 1$ in R is equal to l^{a_l} for each $l \neq p$. Hence Lemma 1 shows that $E(k)$ is equal to $\mathbf{Z}/p^{h_p}\mathbf{Z} \times \prod_{l \neq p}(\mathbf{Z}/l^{a_l}\mathbf{Z} \times \mathbf{Z}/l^{h_l - a_l}\mathbf{Z})$.

Department of Mathematics
University of Arizona
Tucson, Arizona 85721

FB9-Mathematik
Universität des Saarlandes
D-6600 Saarbrücken, West Germany

1. M. DEURING, "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper," *Abh. Math. Sem. Hamburg*, v. 14, 1941, pp. 197–272.

2. J. TATE, "Endomorphisms of abelian varieties over finite fields," *Invent. Math.*, v. 2, 1966, pp. 134–144.

3. J. TATE, *Classes d'Isogénie des Variétés Abéliennes sur un Corps Fini* (*d'après T. Honda*), Séminaire Bourbaki, Exposé 352, Benjamin, New York, 1968/69.

4. W. WATERHOUSE, "Abelian varieties over finite fields," *Ann. Sci. École Norm. Sup.* (4), v. 2, 1969, pp. 521–560.

5. A. WEIL, *Variétés Abéliennes et Courbes Algébriques*, Hermann, Paris, 1948.