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

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with coefficients $a_1, \ldots, a_6$ in $k$. For each field $\bar{k}$ that contains $k$, the set $E(\bar{k})$ of points with coordinates in $\bar{k}$ 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 $k = F_p$) 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 $\beta$ is an integer with $|\beta| \leq 2\sqrt{q}$ 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 $\text{End}(E)$ be the ring of group endomorphisms of $E$ which are given by algebraic equations with coefficients in $k$. It is known that $\text{End}(E)$ is an order in a finite-dimensional division algebra over $Q$. This division algebra determines $#E(k)$:

Theorem 2 [2]. Let $E, E'$ be elliptic curves over $k$; then

$$#E(k) = #E'(k) \quad \text{if and only if} \quad \text{End}(E) \otimes Z Q = \text{End}(E') \otimes Z Q.$$
There is a special endomorphism \( \pi \), 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 \( K = \text{End}(E) \otimes \mathbb{Q} \) 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 \( \beta \) satisfies one of the conditions (a), ..., (e) of Theorem 1a.

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

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

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

Let \( h \) be a possible order and \( h = \prod l^{h_l} \) 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

\[
\mathbb{Z}/p^{h_p} \mathbb{Z} \times \prod_{l \neq p} \left( \frac{\mathbb{Z}}{l^{a_l} \mathbb{Z}} \times \frac{\mathbb{Z}}{l^{h_l-a_l} \mathbb{Z}} \right) \quad \text{with} \quad 0 < a_l < h_l.
\]

The relation between \( \text{End}(E) \) 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 \( \text{End}(E) \).

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

If \( E_m \subseteq E(k) \), 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 \( \lambda \in \text{End}(E) \).

**Lemma 2.** We assume that \( \pi \) is not contained in \( \mathbb{Q} \); 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

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

(\( \lfloor \cdot \rfloor \) is the largest rational integer \( \leq \lambda \); \( v_l(\cdot) \) is the normalized valuation of \( \mathbb{Z} \) corresponding to \( l \)).

**Proof.** The zeta function of \( E \) yields the equation

\[
\#E(k) = (\pi - 1)(\overline{\pi} - 1) = q - (\pi + \overline{\pi}) + 1.
\]
From this we get the two equations

\begin{align}
\#E(k) &= \ell^x \cdot \omega \cdot \overline{\omega} \\
\#E(k) &= (q - 1) - (\pi - 1) - (\overline{\pi} - 1).
\end{align}

If \( \ell \) is prime to \( \omega \), then (3) yields \( 2x = v_\ell(\#E(k)) \) and (4) yields \( v_\ell(q - 1) \geq \min\{x, v_\ell(\#E(k))\} \geq \left\lfloor \frac{v_\ell(\#E(k))}{2} \right\rfloor \).

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

\[ x = \frac{v_\ell(\#E(k)) - 1}{2} = \left\lfloor \frac{v_\ell(\#E(k))}{2} \right\rfloor. \]

Equation (4) shows that \( v_\ell(q - 1) \geq \left\lfloor v_\ell(\#E(k))/2 \right\rfloor \), 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 \( h = \prod_i l_i^{h_i} \) 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:

\[ Z/p^h \times \prod_{l \neq p} (Z/l^{a_i}Z \times Z/l^{a_j - a_i}Z) \]

with

(a) In case (b) of Theorem 1a: Each \( a_i \) is equal to \( h_i/2 \);

(b) In cases (a), (c), (d), (e) of Theorem 1a: \( a_i \) is an arbitrary integer satisfying \( 0 \leq a_i \leq \min\{v_\ell(q - 1), [h_i/2]\} \).

**Proof.** (a) In case (b) of Theorem 1a we get \( \pi \in Z \) and \( h = (\pi - 1)^2 \). Furthermore, \( \pi - 1 \) is divisible by \( m \) in \( \text{End}(E) \) if and only if \( \pi - 1 \) is divisible by \( m \) in \( Z \). Hence Lemma 1 shows that \( a_i = \min\{v_\ell(\pi - 1), [h_i/2]\} = h_i/2 \).

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

\[ \min\{v_\ell(a - 1), v_\ell(b)\} = \min\{v_\ell(q - 1), [h_i/2]\} \]

by Lemma 2. For each \( l \neq p \) let \( a_i \) be arbitrary with

\[ 0 \leq a_i \leq \min\{v_\ell(q - 1), [h_i/2]\}. \]

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

Department of Mathematics
University of Arizona
Tucson, Arizona 85721

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