J.F. Voloch

A note on elliptic curves over finite fields


<http://www.numdam.org/item?id=BSMF_1988__116_4_455_0>
A NOTE ON ELLIPTIC CURVES OVER FINITE FIELDS

BY

J. F. VOLOCH (*)

RÉSUMÉ. — Nous déterminons tous les groupes que l'on peut obtenir comme groupe des points rationnels d'une courbe elliptique sur un corps fini donné.

ABSTRACT. — We determine all groups that can occur as the group of rational points of an elliptic curve over a given finite field.

Let $F_q$ denote the finite field of $q$ elements. Given $t$ an integer, $|t| \leq 2q^{1/2}$ then Waterhouse [3] proved that there exists an elliptic curve over $F_q$ with $q + 1 - t$ rational points if and only if, writing $q = p^h$, $p$ prime, one of the following conditions is satisfied:

(i) $(t, q) = 1$,
(ii) $t = 0$, $h$ odd or $p \neq 1(4)$,
(iii) $t = \pm q^{1/2}$, $h$ even or $p \neq 1(3)$,
(iv) $t = \pm 2q^{1/2}$, $h$ even,
(v) $t = \pm \sqrt{2q}$, $h$ odd and $p = 2$,
(vi) $t = \pm \sqrt{3q}$, $h$ odd and $p = 3$.

Schoof then proved [2] that the possible structures for the group in cases (ii)–(vi) are:

(ii) $\mathbb{Z}/2 \oplus \mathbb{Z}/(q + 1)/2$ or cyclic if $q = 3(4)$, cyclic otherwise,
(iii) Cyclic,
(iv) $(\mathbb{Z}/(q^{1/2} \pm 1))^2$,
(v) Cyclic,
(vi) Cyclic.

The purpose of this paper is to give the list of possibilities for the groups occurring as elliptic curves over $F_q$ in case (i). Let, for a prime $\ell$, $\nu_\ell(n)$ be the largest integer with $\ell^{\nu_\ell(n)} | n$.

THEOREM. — If \( t \) is an integer with \(|t| \leq 2q^{1/2} \) and \( (t,q) = 1 \), the possible groups that an elliptic curve over \( \mathbb{F}_q \) with \( N = q + 1 - t \) can be are

\[
(*) \quad \mathbb{Z}/p^{\nu_p(N)} \oplus \bigoplus_{\ell \neq p} \mathbb{Z}/\ell^{r_\ell} \oplus \mathbb{Z}/\ell^{s_\ell}
\]

with \( r_\ell + s_\ell = \nu_\ell(N) \) and \( \min(r_\ell, s_\ell) \leq \nu_\ell(q - 1) \).

Proof. — Let \( E[n] \) stand for the group of \( n \)-torsion points of an elliptic curve \( E \) over the algebraic closure of \( \mathbb{F}_q \). It is well known that \( E[p] = \{0\} \) or \( \mathbb{Z}/p \) and that \( E[\ell] = (\mathbb{Z}/\ell)^2 \), \( \ell \) prime, \( \ell \neq p \) (see, e.g. [1, Theorem 8.1]).

So, clearly the group of points of an elliptic curve over \( \mathbb{F}_q \) is of the form \((*)\) with \( r_\ell + s_\ell = \nu_\ell(N) \). To see that also \( \min(r_\ell, s_\ell) \leq \nu_\ell(q - 1) \), we notice that, if \( r_\ell \leq s_\ell \), then all points of \( E[\ell^{r_\ell}] \) are defined over \( \mathbb{F}_q \), hence \( \ell^{r_\ell}|q - 1 \) by [2, Proposition 3.8]. It then follows that the conditions of the theorem are necessary. We now prove that they are sufficient. For this we need two lemmas.

LEMMA 1. — Given \( N \not\equiv 1 \pmod{p} \) such that there exists an elliptic curve with \( N \) points over \( \mathbb{F}_q \) then there exists at least one such elliptic curve with its group of rational points being cyclic.

Proof. — Let \( \ell_1, \ldots, \ell_r \) be the primes such that \( \ell_1^2|N \) and \( \ell_i|q - 1 \). If there is no such prime then by the preceding discussion any elliptic curve over \( \mathbb{F}_q \) with \( N \) points will do. So we assume that \( r \geq 1 \).

In [2, Theorem 4.9 (i)], Schoof proves that given an integer \( n \), the number of isomorphism classes of elliptic curves with \( N = q + 1 - t \) points over \( \mathbb{F}_q \) with all points of \( E[n] \) defined over \( \mathbb{F}_q \), when \( p \nmid t \) and \( n^2|N \), \( n|q - 1 \), is \( H(t^2 - 4q)/n^2 \) where \( H(\Delta) \) is the class number of binary quadratic forms of discriminant \( D \) (note that although Theorem 4.9 of [2] its stated only for \( n \) odd the proof of item (i) is valid for all \( n \)). Hence the number \( M \), say, of elliptic curves satisfying the conclusion of the lemma is clearly:

\[
M = H(t^2 - 4q) - \sum_{i=1}^{r} H((t^2 - 4q)/\ell_1^2) + \sum_{1 \leq i < j \leq t} H((t^2 - 4q)/\ell_i^2 \ell_j^2) + \cdots + (-1)^r H((t^2 - 4q)/\ell_1 \cdots \ell_r^2)
\]

\[
H(\Delta) = \sum_{\mathcal{O}(\Delta) \leq \mathcal{O} \leq \mathcal{O}_{\text{max}}} h(\mathcal{O}),
\]

where \( \mathcal{O}(\Delta) \) is the quadratic order of discriminant \( \Delta \), \( h(\mathcal{O}) \) is the class number of \( \mathcal{O} \) and \( \mathcal{O} \) runs through the orders of \( \mathcal{O}(\Delta) \otimes \mathbb{Q} \). It follows that \( M \geq h(\mathcal{O}(t^2 - 4q)) \geq 1 \). The lemma is thus proved.
Définition. — We shall call two elliptic curves $\ell^\infty$-isogenous, for a prime $\ell$, if there exists an isogeny between them of degree a power of $\ell$.

Lemma 2. — If $E$ is an elliptic curve defined over $\mathbb{F}_q$ and $\ell \neq p$ is a prime such that $E$ has a cyclic subgroup of order $\ell^n$, then for any $r \leq s$ with $r + s = n$ and $\ell^r|q - 1$, there exists an elliptic curve defined over $\mathbb{F}_q$, $\ell^\infty$-isogenous to $E$ and containing a subgroup isomorphic to $\mathbb{Z}/\ell^r \oplus \mathbb{Z}/\ell^s$.

Proof. — Let $P \in E$ be a point of order $\ell^n$ in $E$ and let $\Gamma$ be the group generated by $\ell^rP$. Let $E' = E/\Gamma$ and $\lambda : E \to E'$ the natural isogeny [1, Lemma 8.5]. $\lambda$ has degree $\ell^r$, hence is an $\ell^\infty$ isogeny. We shall prove that $E'$ satisfies the conclusions of the lemma. Let $\hat{\lambda}$ be the dual isogeny [1, pg. 216] and $M = \ker \hat{\lambda}$, the points of $M$ are defined over $\mathbb{F}_q$ by [1, Lemma 8.4]. Let $N$ be the group generated by $\lambda(P)$, then $N$ is cyclic of order $\ell^s$ and as $\hat{\lambda} \circ \lambda$ is multiplication by $\ell^r$ [1, 8.7], it follows that $\hat{\lambda}$ is injective on $N$. So $M \cap N = \{0\}$ and as $\#M = \deg \hat{\lambda} = \ell^r$ [1, 8.8] it follows that $M \cong N \cong \mathbb{Z}/\ell^r \oplus \mathbb{Z}/\ell^s$, as desired.

We now complete the proof of the theorem. Take $N \neq 1 \pmod{p}$ and $E$ the elliptic curve given by Lemma 1, so $E(\mathbb{F}_q)$ is cyclic of order $N$. Let $\ell_1, \ldots, \ell_r$ be the primes such that $\ell_i^2 \mid N$ and $\ell_i \mid q - 1$. (If there is no such prime there is nothing to prove). Let $s_1, \ldots, s_r$ be integers with $s_i \leq v_{\ell_i}(N)$ and $v_{\ell_i}(N) - s_i \leq v_{\ell_i}(q - 1)$, $i = 1, \ldots, r$. Construct successively by Lemma 2, elliptic curves $E_1, \ldots, E_r$, with $E_1$ being $\ell_1^\infty$-isogenous to $E$ and containing a subgroup isomorphic to $\mathbb{Z}/\ell_1^{s_1} \oplus \mathbb{Z}/\ell_1^{v_{\ell_1}(N) - s_1}$, $E_r$, $\ell_r^\infty$-isogenous to $E_{r-1}$ and containing a subgroup isomorphic to $\mathbb{Z}/\ell_r^{v_{\ell_r}(N) - s_r}$. Notice that an $\ell^\infty$-isogeny induces an isomorphism between the subgroups of order prime to $\ell$, so the construction is justified since, for $i < r$, $E_i$ has a cyclic subgroup of order $\ell_{i+1}^{v_{\ell_i}(N)}$. Then

$$E_r \cong \mathbb{Z}/p^{v_p(N)} \oplus \bigoplus_{\ell \neq p, \ell_i} \mathbb{Z}/\ell^{v_{\ell}(N)} \oplus \bigoplus_{i=1}^r \mathbb{Z}/\ell_i^{s_i} \oplus \mathbb{Z}/\ell_i^{v_{\ell_i}(N) - s_i}.$$ 

As the $s_i$ were arbitrary satisfying $s_i \leq v_{\ell_i}(N)$ and $v_{\ell_i}(N) - s_i \leq v_{\ell_i}(q - 1)$, the proof of the theorem is complete.

Added in proof. — After this paper was submitted, there appeared in print an article by H. G. RUCH (Math. of Comp., t. 49, 1987, p. 301–304), proving the same result but with a different proof.
REFERENCES

