J.F. VOLOCH

A note on elliptic curves over finite fields

Bulletin de la S. M. F., tome 116, n° 4 (1988), p. 455-458
<http://www.numdam.org/item?id=BSMF_1988__116_4_455_0>

Bull. Soc. math. France,
116, 1988, p. 455–458.

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 $\mathbb{F}_q$ 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 $\mathbb{F}_q$ 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 $p \not\equiv 1(4)$,
(iii) $t = \pm q^{1/2}$, h even or $p \not\equiv 1(3)$,
(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 $\mathbb{F}_q$ in case (i). Let, for a prime ℓ, $v_\ell(n)$ be the largest integer with $\ell^{v_\ell(n)} \mid n$.

(*) Texte reçu le 11 juin 1987, révisé le 14 septembre 1987.
J. F. VOLOCH, IMPA, Estrada Dona Castorina 110, Rio de Janeiro 22460, Brésil.

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE 0037-9484/1988/455/$ 5.00

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*

$$(*) \qquad \mathbb{Z}/p^{v_p(N)} \oplus \bigoplus_{\ell \neq p} \mathbb{Z}/\ell^{r_\ell} \oplus \mathbb{Z}/\ell^{s_\ell}$$

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

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 $E[\ell] = (\mathbb{Z}/\ell)^2$, ℓ 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 $r_\ell + s_\ell = v_\ell(N)$. To see that also $\min(r_\ell, s_\ell) \leq v_\ell(q-1)$, 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 $\ell_i^2 | N$ 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:

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

$$H(\Delta) = \sum_{\mathcal{O}(\Delta) \subseteq \mathcal{O} \subseteq \mathcal{O}_{\max}} h(\mathcal{O}),$$

where $\mathcal{O}(\Delta)$ is the quadratic order of discriminant Δ, $h(\mathcal{O})$ 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.

Definition. — We shall call two elliptic curves ℓ^∞-isogenous, for a prime ℓ, if there exists an isogeny between them of degree a power of ℓ.

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 ℓ^n, then for any $r \leq s$ with $r+s=n$ and $\ell^r | q-1$, there exists an elliptic curve defined over $\mathbb{F}_q$, ℓ^∞-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 ℓ^n in E and let Γ be the group generated by $\ell^s P$. Let $E' = E/\Gamma$ and $\lambda : E \to E'$ the natural isogeny [1, Lemma 8.5]. λ has degree ℓ^r, hence is an ℓ^∞ 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 ℓ^s and as $\hat{\lambda} \circ \lambda$ is multiplication by ℓ^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 $M \oplus N \simeq \mathbb{Z}/\ell^r \oplus \mathbb{Z}/\ell^s$, as desired.

We now complete the proof of the theorem. Take $N \not\equiv 1 \pmod{p}$ 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 $\ell_i^2 | N$ and $\ell_i | q-1$. (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 ℓ_1^∞-isogenous to E and containing a subgroup isomorphic to $\mathbb{Z}/\ell_1^{s_1} \oplus \mathbb{Z}/\ell_1^{v_{\ell_1}(N)-s_1}, \ldots, E_r$, ℓ_r^∞-isogenous to E_{r-1} and containing a subgroup isomorphic to $\mathbb{Z}/\ell_r^{v_{\ell_r}(N)-s_r}$. Notice that an ℓ^∞-isogeny induces an isomorphism between the subgroups of order prime to ℓ, so the construction is justified since, for $i < r$, E_i has a cyclic subgroup of order $\ell_{i+1}^{v_{\ell_{i+1}}(N)}$. Then

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

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

[1] CASSELS (J.W.S.). — Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.*, t. **41**, 1966, p. 193–291.

[2] SCHOOF (R.). — Non-singular plane cubic curves over finite fields, [Ph. D. Thesis], *University of Amsterdam*, 1985, pp. 65–100.

[3] WATERHOUSE (W.C.). — Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup.*, t. **2**, 1969, p. 521–560.