Nova Série
BOLETIM
DA SOCIEDADE BRASILEIRA DE MATEMÁTICA

Bol. Soc. Bras. Mat., Vol. 21, No. 1, 91-94

Primitive points on constant elliptic curves over function fields

J. F. Voloch

Abstract. Let $f: C \to E$ be a non-constant rational map between curves over a finite field, where E is elliptic. We estimate the number of rational points of C whose image under f generate the group of rational points of E.

The Result

A classical conjecture of Artin (see the introduction to [1]) states that given $a \in \mathbb{Q}$, $a \neq 0, 1$, a not a square, then a is a primitive root for infinitely many primes and, in fact, for a positive proportion of the primes. This conjecture of Artin was transposed to the context of elliptic curves by Lang and Trotter [8] as follows: if $E/\mathbb{Q}$ is an elliptic curve with no $\mathbb{Q}$-torsion and $P \in E(\mathbb{Q})$, $P \neq O$ then, for a positive proportion of primes p, P (mod p) generates the group of $\mathbf{F}_p$-rational points of E (mod p).

Artin's conjecture was shown to follow from the generalized Riemann hypothesis by Hooley [7]. (Recent unconditional results were obtained by Gupta and Murty and Heath-Brown, see [4], [6].) Lang-Trotter's conjecture was also shown to follow from the generalized Riemann hypothesis, in the case that E has complex multiplication, by Gupta and Murty [5].

All these conjectures have natural analogues for function fields over finite fields. Since the Riemann hypothesis is known in this context (Weil [11]) one would expect unconditional results. For Artin's conjecture, indeed, Bilharz [2] had proved the analogue of Hooley's result before Weil proved the Riemann hypothesis for function fields. The purpose of this note is to give a proof of the analogue of Lang-Trotter's conjecture for constant elliptic curves over function fields. The

Received 11 March 1990.

non-constant case seems much more difficult and we are not able to say anything about it at present. One of the difficulties is similar to that encountered by Gupta and Murty [5] in the non-CM case in characteristic zero.

We shall formulate our result in a more geometric way, one reason for it is explained in the remark at the end.

Let $\mathbf{F}_q$ be the finite field with q elements and characteristic p.

Theorem. *Let $E/\mathbf{F}_q$ be an elliptic curve with $E(\mathbf{F}_q)$ cyclic and put $N = \#E(\mathbf{F}_q)$. If $C/\mathbf{F}_q$ is an algebraic curve of genus g and $f: C \to E$ is a rational map defined over $\mathbf{F}_q$ which does not factor as $C \to E' \to E$, for any elliptic curve E' then, given any $\varepsilon > 0$,*

$$\#\{P \in C(\mathbf{F}_q) \mid \langle f(P)\rangle = E(\mathbf{F}_q)\} = \varphi(N) + O_\varepsilon(gq^{\frac{1}{2}+\varepsilon}).$$

Proof. For each $\ell | N$ define an elliptic curve $E_\ell/\mathbf{F}_q$ as follows:

(i) $\ell = p$. Let E_ℓ be the image of the $\mathbf{F}_p$ - Frobenius.

(ii) $\ell | (q-1)$. Let Γ_ℓ be the subgroup of $E(\mathbf{F}_q)$ of order ℓ and $E_\ell = E/\Gamma_\ell$.

(iii) $\ell \neq p$. $\ell \nmid (q-1)$. Consider the $\mathbf{F}_q$-Frobenius F,acting on $E[\ell]$, the ℓ-torsion of E, as an element of $GL_2(\mathbb{Z}/\ell\mathbb{Z})$. As $\ell | N$, F has 1 as eigenvalue and therefore it has eigenvalues in $\mathbf{F}_\ell$. The characteristic polynomial of F is $t^2 - at + q$, $a = q + 1 - N$ and since $\ell \nmid (q-1)$, $\ell \neq p$ one sees that the other eigenvalue is different from 0 and 1. Hence there exists a subgroup $\Gamma_\ell \subset E[\ell]$, $\#\Gamma_\ell = \ell$, defined over $\mathbf{F}_q$, but with Γ_ℓ not contained in $E(\mathbf{F}_q)$. Let $E_\ell = E/\Gamma_\ell$.

Let $\lambda_\ell: E_\ell \to E$ be the dual isogeny of the isogeny $\varphi_\ell: E \to E_\ell$ which is given in the construction of E_ℓ. Then $\lambda_\ell: E_\ell \to E$ is of degree ℓ, defined over $\mathbf{F}_q$. Moreover, as we proceed to show, $\lambda_\ell(E_\ell(\mathbf{F}_q)) = \ell E(\mathbf{F}_q)$. As E_ℓ is isogenous to E, $\#E_\ell(\mathbf{F}_q) = N$, so it suffices to show that $\ker \lambda_\ell \subseteq E_\ell(\mathbf{F}_q)$. This is clear in case (i).

In case (ii) it follows from [3], Lemma 8.4.

In case (iii), the dual isogeny $\varphi_\ell: E \to E_\ell$ is injective in $E(\mathbf{F}_q)$, by construction and $\varphi_\ell \circ \lambda_\ell$ is multiplication by ℓ, which is not injective, hence $\ker \lambda_\ell \subset E_\ell(\mathbf{F}_q)$, as desired.

By taking the compositum of the E_ℓ we can define, for any

squarefree $d|N$, an elliptic curve $E_d/\mathbf{F}_q$ with an isogeny $\lambda_d: E_d \to E$ of degree d satisfying $\lambda_d(E_d(\mathbf{F}_q)) = dE(\mathbf{F}_q)$.

Define for any squarefree $d|N$, the curve C_d, compositum of C and E_d. As $C \to E$ was assumed not to factor, it follows that C_d is of degree d over C. It is clear that $P \in C(\mathbf{F}_q)$ satisfies $d \mid [E(\mathbf{F}_q): \langle f(P)\rangle]$ if and only if $f(P) \in dE(\mathbf{F}_q)$. This latter assertion is equivalent to P belong to the image of $C_d(\mathbf{F}_q)$. Moreover, any point in the image of $C_d(\mathbf{F}_q)$ is the image of precisely d points. It follows that

$$M = \#\{P \in C(\mathbf{F}_q) \mid E(\mathbf{F}_q) = \langle f(P)\rangle\} = \sum_{d|N} \mu(d) \# C_d(\mathbf{F}_q)/d.$$

To estimate the cardinality of $C_d(\mathbf{F}_q)$ we use Weil's theorem [11], and for that we need to bound the genus of C_d. As $C_d \to C$ is unramified it follows from Hurwitz's formula that the genus of C_d is at most dg. Hence

$$\begin{aligned} M &= q \sum_{d|N} \mu(d)/d + O\left(\sum_{d|N} |\mu(d)|\, g q^{1/2}\right) \\ &= q\frac{\varphi(N)}{N} + O_\varepsilon(g q^{1/2} N^\varepsilon). \end{aligned}$$

As, by Weil's theorem, $N = q + O(q^{1/2})$, we finally get $M = \varphi(N) + O_\varepsilon(g q^{1/2+\varepsilon})$, as desired.

Remark. To really rephrase the Theorem on a version closer to Lang-Trotter's original conjecture one would have to describe the set $S = \{n \in \mathbf{N} | E(\mathbf{F}_{q^n})$ cyclic$\}$. This seems a difficult question in general. When E is supersingular S can be described as follows (see e.g., [9] lemma 4.8 and Theorem 4.2). Assume $(q, 6) = 1$,

(i) If $N = q + 1 \pm 2q^{1/2}$ then $S = \phi$.

(ii) If $N = q + 1 \pm q^{1/2}$ then $S = \{n \in \mathbf{N}, n \not\equiv 0(3)\}$.

(iii) If $N = q+1$ then $S = \phi$ if $E[2] \subseteq E(\mathbf{F}_q)$ or $S = \{n \in \mathbf{N},\ n \not\equiv 0(2)\}$, otherwise.

In the ordinary case we don't know whether S is infinite, when non-empty, but this seems very likely. All we can say is that there are plenty of ordinary

elliptic curves with cyclic group of rational points, as follows from Lemma 1 of [10].

References

1. Artin E., "Collected papers," Lang, S. and Tate, J. eds., Addison - Wesley, Reading, Mass,, 1965.
2. Bilharz, H., *Primdivisoren mit Vorgegebener Primitivwurzel*, Math. Ann. **114** (1937), 476–492.
3. Cassels, J. W. S., *Diophantine equations with special reference to elliptic curves*, J. Lon. Math. Soc **41** (1966), 193–291.
4. Gupta, R. and Murty, M. R., *A remark on Artin's conjecture*, Inv. Math **78** (1984), 127–130.
5. _____, *Primitive points on elliptic curves*, Compositio Math. **58** (1986).
6. Heath-Brown, D.R., *On Artin's conjecture,*, Quart. J. Math. Oxford **(2)37** (1986), 39–47.
7. Hooley, C., *On Artin's conjecture*, Crelle **225** (1967), 209–220.
8. Lang. S. and Trotter, H., *Primitive points on elliptic curves*, Bull. Amer. Math. Soc. **83** (1977), 289–292.
9. Schoof, R., *Non singular plane cubic curves over finite fields*, J. of Combinatorial theory, Ser A. **46** (1987), 183–211.
10. Voloch, J.F., *A note on elliptic curves over finite fields*, Bull. de la Soc. Math. de France **116** (1988), 455–458.
11. Weil. A., *Sur les courbes algebriques et les varietes que s'en deduisant*, Actualités Sci. Ind. nº 1041,. Hermann, Paris

J. F. Voloch
Instituto de Matemática Pura e Aplicada
Est. D. Castorina, 110
22460, Rio de Janeiro, Brazil