BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 83, Number 2, March 1977

PRIMITIVE POINTS ON ELLIPTIC CURVES

BY S. LANG AND H. TROTTER[1]

Communicated by Olga Taussky Todd, September 23, 1976

A well-known conjecture of Artin predicts the density of primes for which a given rational number is a primitive root (cf. the introduction to his collected works). Our purpose here is to formulate an analogous conjecture on elliptic curves A, say defined over the rationals for concreteness. Let a be a rational point of infinite order. We ask for the density of those primes p such that the group $\bar{A}(\mathbf{F}_p)$ of rational points mod p is cyclic, generated by the reduction $\bar{a}$ of a mod p. We shall use the Galois extensions $K_l = \mathbf{Q}(A_l, l^{-1}a)$ analogous to the splitting fields of the equations $X^l - a = 0$ when a is in the multiplicative group. We may say that *a is primitive* for such primes. We let $\langle a \rangle$ be the cyclic group generated by a.

The affine group, equal to the extension of the translation group A_l by $GL_2(l)$, operates on $l^{-1}a$. For simplicity we fix an element $u_0 \in l^{-1}a$. Then we may represent an element σ in the affine group by a pair (γ, τ) with $\gamma \in GL_2(l)$ and a translation $\tau \in A_l$, such that

$$(\gamma, \tau)u = u_0 + \gamma(u - u_0) + \tau.$$

The Galois group $\mathrm{Gal}(K_l/\mathbf{Q}(A_l))$ can be identified with a group of translations, subgroup of A_l, and is equal to A_l for almost all l by a theorem of Bashmakov [Ba]. If $\sigma = (\gamma, \tau)$ as above, we have

$$\sigma u = u \quad \text{if and only if } (\gamma - 1)(u_0 - u) = \tau.$$

Let Δ be the discriminant of the curve. We want to give a condition on the Frobenius element $\sigma_p = (\gamma_p, \tau_p)$ in G_l when $p \nmid \Delta l$ in order that the index of $\langle \bar{a} \rangle$ in $\bar{A}(\mathbf{F}_p)$ is divisible by l. Note that l divides the order of $\bar{A}(\mathbf{F}_p)$ if and only if γ_p has eigenvalue 1. Furthermore, $\bar{A}(\mathbf{F}_p) = \mathrm{Ker}(\gamma_p - 1)$.

If $\gamma_p = 1$ then the index of $\langle \bar{a} \rangle$ is divisible by l.

Suppose on the other hand that $\mathrm{Ker}(\gamma_p - 1)$ is cyclic of order l. Then the index of $\langle \bar{a} \rangle$ is divisible by l if and only if there exists $b \in \bar{A}$ with $lb = \bar{a}$ and b is fixed by σ_p. Indeed, if $\bar{a}$ has period divisible by l, and the index is divisible by l, then $\bar{a}$ is divisible by l in $\bar{A}(\mathbf{F}_p)$, otherwise $\bar{A}(\mathbf{F}_p)$ would contain $\mathbf{Z}(l)^2$. The converse is clear. If $\bar{a}$ has period not divisible by l then $lb = \bar{a}$ for some b in $\langle \bar{a} \rangle$, so the assertion is also clear in this case.

We see that *the index of $\langle \bar{a} \rangle$ is divisible by l if and only if σ_p lies in the*

AMS (MOS) subject classifications (1970). Primary 12A75, 14G25.
[1]Both authors supported by NSF grants.

set S_l' consisting of all elements (γ, τ) such that γ has eigenvalue 1, and either $\gamma = 1$, or $\mathrm{Ker}(\gamma - 1)$ is cyclic and $\tau \in \mathrm{Im}(\gamma - 1)$.

Let $S_l = G_l - S_l'$. For any set of primes L we let $S_L = \Pi_{l \in L} S_l$. We let K_L be the compositum of all fields K_l with $l \in L$, and $G_L = \mathrm{Gal}(K_L/\mathbf{Q})$. We let $P_{L,S}(x)$ be the set of primes $p \leqslant x$ such that $p \nmid \Delta$ and the Frobenius element $(p, K_l/\mathbf{Q}) \in S_l$ for all $l \in L$ and $l \neq p$. If L is finite, we have by Tchebotarev,

$$\lim_{x \to \infty} \frac{|P_{L,S}(x)|}{\pi(x)} = \frac{|S_L \cap G_L|}{|G_L|} = \delta_L(S).$$

It is easy to see that the limit $\delta(S) = \mathrm{Lim}_L \delta_L(S)$ exists (for L increasing to include all primes). The conjecture states that the limit is equal to the density of primes for which a is primitive.

There exists a finite set M of primes such that for any L containing M we have

$$\delta_L = \delta_M \prod_{l \in L - M} \delta_l, \quad \text{where} \quad \delta_l = 1 - \frac{|S_l' \cap G_l|}{|G_l|}.$$

This allows for effective computation of the conjectured density. One finds in all cases that $\delta_l = 1 + O(1/l^2)$, so that the product is absolutely convergent. When there is no complex multiplication, for instance, and G_l is the full affine group (which occurs for almost all l), then one finds

$$\delta_l = 1 - \frac{|S_l'|}{|G_l|} \quad \text{where} \quad \frac{|S_l'|}{|G_l|} = \frac{l^3 - l - 1}{l^2(l^3 - l^2 - l + 1)}.$$

We have computed numerical values for some "Serre curves" (cf. **[LT]**) whose Galois group of torsion points is of index 2 in the full product of all $GL_2(\mathbf{Z}_l)$, for instance the three curves

$$y^2 + y = x^3 - x, \quad y^2 + y = x^3 + x^2, \quad y^2 + xy + y = x^3 - x^2.$$

In each case the point of infinite order is the point (0, 0), and the predicted density comes within three decimals of 0.440. Among the first 200 primes, the expected number is then 88, and the actual numbers are 91, 96, 91 respectively. For 180 primes (leaving out the first 20) the expected number is 79.2, and the actual numbers are 79, 84, 78 respectively, a good fit. One can of course handle in a similar way the density of primes p such that $\bar{A}(\mathbf{F}_p)$ is cyclic (forget about a).

We have also considered the more general problem dealing with a free subgroup Γ of rational points, rather than an infinite cyclic one. Let M be an integer > 1. We wish to characterize the possibility that the image under reduction

$$\Gamma \longrightarrow \bar{A}(\mathbf{F}_p)/M\bar{A}(\mathbf{F}_p)$$

is surjective by a condition on the Frobenius element σ_p. For simplicity, fix a section $\lambda\colon \Gamma \longrightarrow M^{-1}\Gamma$ such that $M\lambda a = a$ for all $a \in \Gamma$. This corresponds to choosing u_0 when Γ is infinite cyclic, and determines a homomorphism $\tau\colon \Gamma \longrightarrow A_M$ such that

$$\sigma u = \gamma(u - \lambda u) + \lambda Mu + \tau Mu$$

for $u \in M^{-1}\Gamma$. We can identify an element σ of the affine group in this case with a pair (γ, τ). We see this time that $\sigma u = u$ if and only if $(\gamma - 1)(u - \lambda Mu) = -\tau Mu$. If we let T_p be the kernel of the map

$$\Gamma \longrightarrow \bar{A}(\mathbf{F}_p)/M\bar{A}(\mathbf{F}_p),$$

then $T_p = \tau_p^{-1}((\gamma_p - 1)A_M)$, where $\sigma_p = (\gamma_p, \tau_p)$ is the Frobenius element. Note that we have an equality of indices

$$(\bar{A}(\mathbf{F}_p)\colon MA(\mathbf{F}_p)) = |(\bar{A}(\mathbf{F}_p) \cap \bar{A}_M)| = |\mathrm{Ker}\,(\gamma_p - 1)|.$$

In particular, take $M = l$ prime. We find:

The index of $\overline{\Gamma}$ in $\bar{A}(\mathbf{F}_p)$ is prime to l if and only if

$$\dim \tau(\Gamma) - \dim(\tau(\Gamma) \cap \mathrm{Im}(\gamma - 1)) = \dim \mathrm{Ker}(\gamma - 1).$$

We define the bad set S_l' to consist of those $\sigma = (\gamma, \tau)$ such that either $\mathrm{Ker}(\gamma - 1)$ is cyclic and $\tau(\Gamma) \subset \mathrm{Im}(\gamma - 1)$, or $\mathrm{Ker}(\gamma - 1) = A_l$ and rank $\tau(\Gamma) =$ 0 or 1. Then we obtain:

The index of $\overline{\Gamma}$ in $\bar{A}(\mathbf{F}_p)$ is divisible by l if and only if the Frobenius element σ_p lies in S_l' (for $p \nmid \Delta l$).

The same type of limit as before yields the conjectured density of primes such that $\overline{\Gamma} = \bar{A}(\mathbf{F}_p)$, (say for which Γ is primitive).

Trying to prove the conjecture from the Riemann hypothesis in line with Hooley's work for the Artin case [H] met difficulties having to do with the larger degrees, behaving like $>><< l^6$ (or l^4 in the complex multiplication case) rather than l^2 in the Artin case. It also leads to the problem of proving the analogue of the Brun-Titchmarsh theorem, to given an upper bound for the number of primes $p \leqslant x$ such that the Frobenius at p operating on A_l has eigenvalue 1.

BIBLIOGRAPHY

[Ba] M. I. Bašmakov, *Un théorème de finitude sur la cohomologie des courbes élliptiques*, C. R. Acad. Sci. Paris Sér. A–B **270** (1970), A999–A1101. MR **42** #4548.

[Go] L. Goldstein, *Analogues of Artin's conjecture*, Trans. Amer. Math. Soc. **149** (1970), 431–442. MR **43** #4792.

[Ho] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220. MR **34** #7445.

[LT] S. Lang and H. Trotter, *Frobenius distributions in GL_2-extensions*, Lecture Notes in Math., vol. 504, Springer-Verlag, Berlin and New York, 1975.

[We] P. Weinberger, *A counterexample to an analogue of Artin's conjecture,* Proc. Amer. Math. Soc. **35** (1972), 49–52. MR **45** #8630.

DEPARTMENT OF MATHEMATICS, YALE UNIVERSITY, NEW HAVEN, CONNECTICUT 06520

DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, PRINCETON, NEW JERSEY 08540