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.