ON THE RANK OF ELLIPTIC CURVES

MATHEMATICS

1967

SovietRxiv

Abstract

Full Text

UDC 513.6

MATHEMATICS

J. T. TATE, Corresponding Member of the Academy of Sciences of the USSR, and I. R. SHAFAREVICH

ON THE RANK OF ELLIPTIC CURVES

Let k be a finite field, $K = k(t)$, and let A be an elliptic curve defined over K. The purpose of this note is to show that the rank of the group of rational points A_K can take arbitrarily large values with a suitable choice of the curve A and a fixed field K. Over the field $k(t)$, where k is an algebraically closed field of characteristic 0, analogous examples were constructed by A. I. Lapin ([1]).

We begin with the construction of simpler examples in which the field K will not be fixed. Denote by k_f the field of p^f elements and by $\bar{k}$ the algebraic closure of any of the fields k_f. Let C be a geometrically irreducible complete curve, and let A be an elliptic curve, both defined over the field k. Considering A as a curve over the field $L = k(C)$, denote by r the rank of the group A_L. As is well known, r coincides with the rank of the group $\mathrm{Hom}_k(J(C), A)$, where $J(C)$ is the Jacobian variety of the curve C. Denote by $P_C(U)$ and $P_A(U)$ the numerators of the ζ-functions $Z_C(U)$ and $Z_A(U)$ of the curves C and U. From the results of ([2]) it follows (Theorem 1) that

$$r = 2h, \tag{1}$$

if $P_C = P_A^h \cdot G$ and P_A is irreducible over Q, or $P_C = P_A^{h/2} \cdot G$ and $P_A = F^2$, where $(P_A, G) = 1$.

In connection with this we shall begin with the explicit computation of the polynomial $P_C(U)$ for some curves C.

Theorem 1. Let C be a complete nonsingular model of the curve defined over k_1 by the equation

$$y^e = \gamma x^f + \delta,$$

where the following conditions are satisfied: $\gamma\delta \in k_1^*$, $p \nmid ef$, $2 \leq e \leq f$, $m = \mathrm{l.c.m.}(e, f)$ divides $p^n + 1$ for some n. Denote by G the direct product of cyclic groups $\{\xi\}$ and $\{\eta\}$ of orders e and f, and for $\varphi \in \mathrm{Hom}(G, \bar{k}^*)$ put $k_\varphi = k_1(\varphi(\xi), \varphi(\eta))$, $d_\varphi = [k_\varphi : k_1]$. If

$$\varphi(\xi) \neq 1, \qquad \varphi(\eta) \neq 1, \qquad \varphi(\xi\eta) \neq 1, \tag{2}$$

then the number d_φ is even: $d_\varphi = 2c_\varphi$, and

$$P_C(U) = \prod (1 + p^{c_\varphi} U^{d_\varphi}), \tag{3}$$

where the product is extended over all φ satisfying condition (2), and from each class of homomorphisms conjugate with respect to the action of the Galois group of the field k_φ/k_1 only one representative is taken.

We shall use the results of ([3]), some of which we recall for the reader' s convenience.

Introduce the following notation: ζ is a primitive m-th root of unity in $\bar{k}$;

$$\varphi(\xi) = \zeta^{maf^{-1}}; \qquad \varphi(\eta) = \zeta^{mbf^{-1}};$$

m_φ is the order of φ; $a_0 = m_\varphi a f^{-1}$; $b_0 = m_\varphi b f^{-1}$; w is a generator of the group k_φ^*, chosen so that

$$\zeta^{m m_\varphi^{-1}} = w^{(p^{d_\varphi}-1)m_\varphi^{-1}}$$

and χ is a character of the group k_φ^* such that $\chi(w) = e^{2\pi i m_\varphi^{-1}}$.

In this notation, the formulas given on p. 493 (3) give

$$P_C(U) = \prod L_\varphi(U),$$

where φ runs through the same values as in (3), and

$$L_\varphi(U) = 1 + \chi\left((\gamma^{-1}\delta)^{a_0}(-\delta)^{b_0}\right) j U^{d_\varphi}; \tag{4}$$

$$j = \sum_{x+y+1=0} \chi(x)^{a_0}\chi(y)^{b_0}, \qquad x, y \in k_\varphi^*. \tag{5}$$

Since m_φ is the least common multiple of the orders of $\varphi(\xi)$ and $\varphi(\eta)$ in the group k_φ^*, we have $k_\varphi = k_1(\zeta^{m m_\varphi^{-1}})$, and d_φ is the least integer for which $m_\varphi \mid (p^{d_\varphi} - 1)$. Thus, in the group $(\mathbb{Z}/m_\varphi\mathbb{Z})^*$ the element $p + m_\varphi\mathbb{Z}$ has order d_φ, while $p^n + m_\varphi\mathbb{Z}$ has order 2, since $m_\varphi \mid m$, by hypothesis $m \mid (p^n + 1)$, and $m_\varphi > 2$ in view of (2). Hence it follows easily that $d_\varphi = 2(n, d_\varphi)$ and, in particular, d_φ is even. We also see that

$$p^{c_\varphi} \equiv p^n \equiv -1 \pmod{m_\varphi}, \qquad c_\varphi = d_\varphi/2. \tag{6}$$

Let us note that $\chi = 1$ on $k^*_{c_\varphi}$. Indeed, $k^*_{c_\varphi} = \{w^{p^{c_\varphi}+1}\}$, and

$$\chi\left(w^{p^{c_\varphi}+1}\right) = e^{(2\pi i m_\varphi^{-1})(p^{c_\varphi}+1)} = 1$$

by (6). In particular, $\chi = 1$ on $k^*_{c_\varphi}$.

We shall now prove that in our case

$$j = p^{c_\varphi}, \tag{7}$$

where j is the Jacobi sum defined by equality (5). For this we use the relation

$$j = p^{-d_\varphi} g(a_0)g(b_0)g(-a_0-b_0) \tag{8}$$

((3), formula 7), where $g(r)$ is a Gauss sum:

$$g(r) = \sum_{x \in k^*_\varphi} \chi(x)^r \psi(x),$$

and ψ is the standard character of the additive group of the field k_φ. We shall prove that

$$g(r) = \chi(c)^r p^{c_\varphi}, \tag{9}$$

if $r = a_0, b_0$ or $-a_0, -b_0$ and $c \in k^*_{d_\varphi}$ is an element whose trace with respect to the subfield k_{c_φ} is equal to 0. It is clear that (7) follows from (8) and (9). Formula (9) follows from the following lemma with $k = k_{d_\varphi}$, $k_0 = k_{c_\varphi}$, since, in view of (2), $m \nmid r$ and hence χ^r is nontrivial on $k^*_{d_\varphi}$.

Lemma. Let k be a quadratic extension of a finite field k_0 of q elements; let θ be a non-unit character of the group k^*, trivial on k_0^*, and let ψ be the standard additive character of k. Then

$$\sum_{x \in k^*} \theta(x)\psi(x) = \theta(c)q,$$

where $c \in k^*$ is such that $\mathrm{Tr}_{k/k_0}(c) = 0$.

Let

$$k^* = \bigcup a_i k_0^*$$

be the decomposition of k^* into cosets modulo k_0^*. Since $\theta = 1$ on k_0^*, we have

$$\sum_{x\in k^*} \theta(x)\psi(x) = \sum_i \theta(a_i) \sum_{y\in k_0^*} \psi(a_i y).$$

But

$$\sum_{y\in k_0^*} \psi(a_i y) = \sum_{y\in k_0} \psi(a_i y) - 1 = \begin{cases} -1, & \text{if } \psi \neq 1 \text{ on } a_i k_0, \\ q-1, & \text{if } \psi = 1 \text{ on } a_i k_0. \end{cases}$$

We also use the fact that $\sum_i \theta(a_i) = 0$, since $\theta \neq 1$ on k^*/k_0^*. We obtain that

$$\sum_{x\in k^*} \theta(x)\psi(x) = \left(\sum_i \theta(a_i)\right) q, \tag{10}$$

where the sum is extended over those i for which $\psi = 1$ on $a_i k_0$. Such an a_i is, in particular, the element c: in view of the definition of the character ψ,

$$\psi(cy) = \psi_1(\mathrm{Tr}_{k/k_1}(cy)),$$

where ψ_1 is a character of the group k_1, and

$$\mathrm{Tr}_{k/k_1}(cy) = \mathrm{Tr}_{k_0/k_1}(\mathrm{Tr}_{k/k_0}(cy)), \qquad \mathrm{Tr}_{k/k_0}(cy) = 0$$

in view of the choice of c.

On the other hand, two distinct terms a_i and a_j cannot enter the sum (10), since otherwise ψ would be trivial on $k = a_i k_0 + a_j k_0$, which is not so. This proves the lemma and (9). Since, moreover, $\chi = 1$ on k_1^*, while $\gamma, \delta \in k_1^*$, it follows that $L_\varphi = 1 + p^{c_\varphi} U^{d_\varphi}$, which proves (3).

Suppose now that the relation $m \mid (p^n+1)$ holds for no n. Then from the relation $d_\varphi = 2(n, d_\varphi)$ it follows that c_φ is odd and each of the factors $L_\varphi(U)$ is divisible by $1 + pU^2$. As is known, $1 + pU^2 = P_A(U)$, where A is a supersingular elliptic curve defined over the field k_1. Therefore, in the case under consideration the number h in formula (1) is equal to the number of all classes of homomorphisms φ satisfying condition (2). In particular, if $e = 2$, then this number is equal to the number of divisors of the polynomial $x^f - 1$ irreducible over k_1 and distinct from $x - 1$, and, when $2 \mid f$, from $x + 1$. Thus we have the following.

Corollary. *If A is a supersingular elliptic curve defined over the field k_1, C is defined by the equation*

$$y^2 = \gamma x^f + \delta, \tag{11}$$

where $f \mid (p^n+1)$, $2 \nmid n$, $p \neq 2$, *then the rank of the curve* A *over the field* $k_1(C)$ *is equal to* $2h$, *where* h *is the number of divisors irreducible over* k_1 *of the polynomial* $x^f - 1$, *distinct from* $x-1$ *and, when* $2 \mid f$, *from* $x+1$.

Let us note that there always exists a supersingular curve A defined over the field k_1. For this it is enough, in view of the results of [4], to show that p is the norm of an integral element of the quaternion algebra $\mathfrak{A}$ over Q, ramified only at p and ∞. But if $p \equiv -1(4)$, then $\mathfrak{A} = (-p, -1)$, while if $p \equiv 1(4)$, then $\mathfrak{A} = (-p, -q)$, where q is a prime number, $q \equiv -1(4)$, $(q/p) = -1$. In both cases $\mathfrak{A}$ contains an element u such that $u^2 + p = 0$.

We now turn to the construction of a curve defined over the field $k_1(x)$. For this, on the curve C given by equation (11), consider the automorphism s: $s(x) = x$, $s(y) = -y$, and on the surface $C \times A$ the automorphism $\sigma(c, a) = (s(c), -a)$, $c \in C$, $a \in A$. The projection $C \times A \to C$ defines a map $(C \times A)/\sigma \to C/s = \mathbf{P}^1$. Therefore we may regard the field $\mathcal{K} = k_1(V)$, $V = (C \times A)/\sigma$, as a field of transcendence degree 1 over the field $k_1(\mathbf{P}^1) = k_1(x)$.

It is easy to see that the genus of the field $\mathcal{K}/k_1(x)$ is 1.

If the curve A is given by the equation $v^2 = u^3 + au^2 + bu + c$, then the field $\mathcal{K}/k_1(x)$ is the field of rational functions on the curve given by the equation

$$v^2 = u^3 + a(\gamma x^f + \delta)u^2 + b(\gamma x^f + \delta)^2 u + c(\gamma x^f + \delta)^3. \tag{12}$$

The rank of curve (12) over $k_1(x)$ is, as is easy to see, equal to the rank of the group of such maps, defined over k_1, $f : C \to A$, that

$$f(c^s) = -f(c). \tag{13}$$

For any map $f : C \to A$, the map $c \to f(c) + f(c^s)$ is constant, since it is equal to the composition of the map $C \to \mathbf{P}^1$ and a certain map $\mathbf{P}^1 \to A$. From the fact that the group A_{k_1} is finite, it follows that the group of maps satisfying (13) has finite index in the group of points of A rational over $k_1(C)$. Therefore the rank of curve (12) over $k_1(x)$ is equal to the rank of the curve A over $k_1(C)$, which is determined by Theorem 1 and the corollary. Thus we have proved

Theorem 2. *The rank of curve (12) over the field* $k_1(x)$, *for* $f \mid (p^n+1)$, $2 \nmid n$, $p \neq 2$, *is equal to* $2h$, *where* h *is the number of irreducible divisors over* k_1 *of the polynomial* $x^f - 1$ *distinct from* $x-1$ *and for* $2 \nmid f$ *also from* $x+1$.

Suppose, in particular, that $f = p^n + 1$ and n is a prime number. Then the number of irreducible divisors of the polynomial $x^f - 1$ distinct from $x+1$ is, as is easy to verify, $(p^n - p)/2n + (p-1)/2$, and we see that the rank of curve (12) over the field $k_1(x)$ for $f = p^n + 1$, $p \neq 2$, and n prime is equal to $(p^n - p)/n + p - 1$.

Thus the rank can assume arbitrarily large values.

Institute for Advanced Scientific Studies
Paris, France

Harvard University
USA

V. A. Steklov Mathematical Institute
Academy of Sciences of the USSR

Received
3 V 1967

CITED LITERATURE

[1] A. I. Tashin, Izv. AN SSSR, ser. matem., 28, 953 (1964).
[2] J. Tate, Inventiones Math., 2, No. 2, 134 (1966).
[3] A. Weil, Trans. Am. Math. Soc., 73, No. 3, 487 (1952).
[4] M. Deuring, Abh. Math. Sem. Hamburg, 14, 197 (1941).

Note: Figure translations are in progress. See original paper for figures.