

## On Hasse Principle for $x^n = a$

By Takashi ONO<sup>\*)</sup> and Tomohide TERASOMA<sup>\*\*)</sup>

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1997)

**Introduction.** Let  $k$  be a number field,  $a$  a nonzero number in  $k$  and  $n$  an integer  $> 1$ . By the Hasse principle for  $x^n = a$  we mean of course the following

(0.1) **Theorem.** *The equation  $x^n = a$  has a solution  $x$  in  $k$  if and only if it has a solution  $x_v$  in  $k_v$  for every place  $v$  of  $k$ .*

In view of the isomorphism

$$(0.2) \quad k^\times/k^{\times n} \cong H^1(k, \mu_n), \text{ (similarly for } k_v),$$

(0.1) is equivalent to the vanishing of the Shafarevich-Tate group:

$$(0.3) \quad \text{III}(k, \mu_n) = \text{Ker} \{H^1(k, \mu_n) \rightarrow \prod_v H^1(k_v, \mu_n)\} = 0.$$

Let  $E = (E, 0)$  be an elliptic curve over  $k$ .<sup>1)</sup> Then we have

$$(0.4) \quad \text{Aut}(E) \cong \mu_n, \quad n = 2, 4 \text{ or } 6.$$

From (0.2) and (0.4), it follows that

$$(0.5) \quad \text{Twist}(E/k) = H^1(k, \text{Aut}(E)) \cong k^\times/k^{\times n},$$

(similarly for  $k_v$ ). Since, up to  $\bar{k}$ -isomorphisms, elliptic curves are in one-to-one correspondence with invariants  $j(E) \in k$ , (0.3) and (0.5) imply the following Hasse principle for elliptic curves over  $k$ .

(0.6) **Corollary to (0.1).** *Let  $E, E'$  be elliptic curves over  $k$ . Then  $E \cong E'$  over  $k$  if and only if  $E \cong E'$  over  $k_v$  for all  $v$ .*

(0.7) **Comments.** Theorem 1 on p. 96 of [1] involving a finite set  $S$  of primes in  $k$  contains our (0.1) as a special case. The “ $S$ -version” of (0.1) goes like this. Let  $S$  be a finite set of places of  $k$  including all archimedean places but excluding some prime factor in  $k$  of each prime factor of  $n$ . Then  $x^n = a$  has a solution in  $k$  if it has a solution in  $k_p$  for every  $p \notin S$ . Although (0.1) is a special case of the theorem quoted above, we submit this paper for publication, as our proof is somehow different from their proof.

**1. Proof of (0.1).** As is easily seen, we

---

<sup>\*)</sup> Department of Mathematics, The Johns Hopkins University, U. S. A.

<sup>\*\*)</sup> Department of Mathematical Sciences, University of Tokyo.

1) As for standard facts on elliptic curves, see [2].

have only to prove the theorem for  $n = \ell^e$ ,  $\ell$  being a prime. So we assume that  $n = \ell^e$  although this is really needed only at the last stage of the proof. Choose a number  $b \in \bar{k}$ , the algebraic closure of  $k$ , so that  $b^n = a$ . Let  $z$  be a primitive  $n^{\text{th}}$  root of unity. Then  $K = k(b, zb, \dots, z^{n-1}b) = k(z, b)$  is a Galois extension of  $k$ , as being the splitting field of  $x^n - a \in k[x]$ . For each  $\sigma \in \text{Gal}(K/k)$ , an ordered pair  $(t, u) \in \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$  is determined so that

$$\sigma z = z^t, \quad \sigma b = z^u b.$$

Setting

$$\phi[\sigma] = \begin{pmatrix} t & u \\ 0 & 1 \end{pmatrix},$$

one obtains an injective homomorphism

$$\phi: \text{Gal}(K/k) \rightarrow GL_2(\mathbf{Z}/n\mathbf{Z}).$$

Call  $G$  the image of  $\phi$ . If we put

$$B = \left\{ \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbf{Z}/n\mathbf{Z}) \right\}, \quad N = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \in B \right\},$$

then  $G \subset B$  and we have

$$(1.1) \quad G/G \cap N \hookrightarrow B/N \cong (\mathbf{Z}/n\mathbf{Z})^\times.$$

By the assumption in (0.1), for each  $p$  in  $k$  and each prime  $\rho$  in  $K$  lying above  $p$ , there is an  $i$  so that  $z^i b \in K \cap k_\rho \subset K\rho$ . Let  $D\rho$  be the subgroup of  $\text{Gal}(K/k)$ , the decomposition group of  $\rho$ , corresponding to the intermediate field  $K \cap k_\rho$  of  $K/k$ . Consequently,

$$(1.2) \quad D\rho \text{ stabilizes } z^i b \text{ for some } i \in \mathbf{Z}/n\mathbf{Z}.$$

If, in particular,  $\rho$  is unramified for  $K/k$ , then  $\text{Frob } \rho$ , a generator of  $D\rho$ , stabilizes  $z^i b$ . Back to the situation (1.1), we claim that

$$(1.3) \quad G \cap N = 1.$$

In fact, let  $g = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$  be any element of  $G \cap N$ . It can also be written  $g = \phi(\sigma) = \begin{pmatrix} t & u \\ 0 & 1 \end{pmatrix}$ ,

$\sigma \in \text{Gal}(K/k)$ . Comparing two matrices, we have  $t = 1, u = c$ . On the other hand, by Chebotarev theorem, one finds a prime  $\rho$  in  $K$  such that  $\sigma = \text{Frob } \rho$ . In view of (1.2), there is an  $i$  so that  $z^i b = \sigma(z^i b) = z^{ti+u} b = z^{i+c} b$ ; hence  $c = 0$ , and so  $g = 1$ .

Now let  $H$  be the subgroup of  $\text{Gal}(K/k)$  corresponding to the field  $k(z)$ , the cyclotomic subfield of  $K$ . Then, we have, by (1.3),