ON THE SOLUTIONS OF THUE EQUATIONS (Analytic Number Theory)

Author(s)
FUJIMORI, MASAMI

Citation
数理解析研究所講究録 (1996), 958: 56-58

Issue Date
1996-08

Type
Departmental Bulletin Paper

URL
http://hdl.handle.net/2433/60466
ON THE SOLUTIONS OF THUE EQUATIONS

MASAMI FUJIMORI

Let $k/\mathbb{Q}$ be a finite extension, $p(X,Y) \in k[X,Y]$ a homogeneous polynomial of degree $n > 3$ with non-zero discriminant, and $a \in k^{\times} = k \setminus \{0\}$. The equation

$$p(X,Y) = aZ^n$$

defines a regular curve $C$ in $\mathbb{P}_k^2$ of genus $g = (n-1)(n-2)/2$.

Here we obtain an estimate for the number of integral solutions and a certain information about rational points.

Remark 0.1. In [2], we required that $p(X,Y)$ be divisible by a linear element in $k[X,Y]$, but it is easily seen we do not have to assume that. The same results follow if we replace the map $f^a$ there by the map $f: C \rightarrow J = \text{the Jacobian of } C$,

$$C(\bar{k}) \ni P \mapsto \mathcal{O}_C(2g-2)P - \text{a canonical divisor} \in \text{Pic}^0(C_{\bar{k}}) \simeq J(\bar{k})$$

which is defined over $k$, noting that this map equals $2g-2$ times $f^a$.

1. INTEGRAL SOLUTIONS

For simplicity, we state the result only in the case of rational integral solutions. As for the algebraic $S$-integer version, we refer the reader to [2, Theorem 5.4].

In this section we assume that $a$ and the coefficients of $p(X,Y)$ are in $\mathbb{Z}$.

In 1983, Silverman used the Jacobian variety $J$ of $C$ to estimate the number of integral solutions from above:

**Theorem 1.1 (Silverman [4]).** If all the exponents of prime factors of $a$ are less than $n$, and $|a|$ is sufficiently large, then

$$\# \{(x,y) \in \mathbb{Z}^2 \mid p(x,y) = a\} < n^{2n^2}(8n^3)^R,$$

where $R = \text{rank } J(\mathbb{Q})$.

1991 *Mathematics Subject Classification.* Primary 11D41; Secondary 11G30.
We can think of $J(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$ as a Euclidean space with some height function. He mapped $C(\mathbb{Q})$ to $J(\mathbb{Q})$ and counted the number of lattice points which lie in a ball of $J(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$.

On the other hand, Mumford had asserted in 1965 paper [3] that in general, the heights of rational points on the Jacobian which come from a curve under a certain map increase at least exponentially if the genus is greater than 1.

Putting the above two results together, we obtain

**Theorem 1.2.** If all the exponents of prime factors of $a$ are less than $n$, and $|a|$ is sufficiently large, then

$$
\#\{(x, y) \in \mathbb{Z}^2 \mid p(x, y) = a\} \leq 4 \cdot 7^R,
$$

where $R = \text{rank } J(\mathbb{Q})$.

### 2. Rational Points

For a general curve $C$ over $k$ of genus $g > 1$, there is a result of Vojta about the distribution of the rational points of $C$ in the Jacobian variety $J$.

Let $\langle \cdot, \cdot \rangle$ and $\|\cdot\|$ be respectively the inner product and the norm on $J(k) \otimes_{\mathbb{Z}} \mathbb{R}$ induced by the Néron-Tate height attached to the $\Theta$-divisor.

**Theorem 2.1 (Vojta [5], cf. [1]).** Assume $C(k) \neq \emptyset$. Regard $C \subset J$ by an appropriate map. For $\varepsilon > 0$, there exists a constant $\gamma = \gamma(C, \varepsilon)$ such that if $P, Q \in C(k)$ satisfy the inequalities $\|P\| > \gamma$ and $\|Q\| > \gamma\|P\|$, then

$$
\langle P, Q \rangle / \|P\| \|Q\| < 1 / \sqrt{g} + \varepsilon.
$$

If we have a non-trivial automorphism of the curve, what can we say about the distribution of the rational points of the curve? When asking this question, we prefer to use the morphism $f : C \to J$ given by

$$
C(\overline{k}) \ni P \mapsto \mathcal{O}_C((2g - 2)P - a) \text{ a canonical divisor} \in \text{Pic}^0(C_{\overline{k}}) \cong J(\overline{k}),
$$

where $\overline{k}$ is an algebraic closure of $k$ and $C_{\overline{k}} = C \times_k \text{Spec } \overline{k}$. Automorphisms of $C$ induce norm preserving morphisms of $J$ compatible with the above map. In other words, there exists a canonically defined representation of $\text{Aut}_k C$ on the Euclidean space $(J(k) \otimes_{\mathbb{Z}} \mathbb{R}, \|\cdot\|)$ which leaves the image of $C(k)$ stable.

In the case of Thue curves, we obtain the following result: Let $C$ be the Thue curve as before. For an $n$-th root $\zeta$ of unity in $k$, we have an automorphism of $C$ defined as

$$
C(\overline{k}) \ni P = (x : y : z) \mapsto P_{\zeta} := (x : y : \zeta z) \in C(\overline{k}).
$$
Proposition 2.2. For $P \in C(k)$, if $\zeta \neq 1$ and $\|fP\| \neq 0$, then
\[
(f_{\zeta}, fP)/\|f_{\zeta}\| \|fP\| = -1/(n - 1).
\]

As an application of this kind of results, if $C$ is a twisted Fermat curve of degree 4, for example, we can see the rational points lie in an intersection of quadric hypersurfaces in $J(k) \otimes_{\mathbb{Z}} \mathbb{R}$. The author will explain it elsewhere.

REFERENCES


MATHEMATICAL INSTITUTE, FACULTY OF SCIENCE, TOHOKU UNIVERSITY, SENDAI 980-77, JAPAN