Tôhoku Math. J.
45 (1993), 311–329

ON RATIONAL POINTS OF CURVES OF GENUS 3 OVER FINITE FIELDS

TOMOYOSHI IBUKIYAMA*

(Received January 29, 1992, revised September 9, 1992)

Abstract. Let F be any finite field with q elements such that q is the square of an odd prime. For each extension F' of odd (resp. even) degree over F, we shall show that there exists a curve of genus 3 defined over F' such that the number of F'-rational points attains the maximum (resp. minimum) of the Weil estimation.

For any curves C defined over finite fields $\boldsymbol{F}_q$ ($q=p^d$; p : prime), Weil [20] gave an estimate for the cardinality of the set $C(\boldsymbol{F}_q)$ of $\boldsymbol{F}_q$-rational points of C as follows:

$$|\sharp(C(\boldsymbol{F}_q))-1-q|\le 2g\sqrt{q}$$

where $g=g(C)$ is the genus of the curve C. When q is a square, for a fixed q and variable g, very interesting phenomena occur and the upper bound and asymptotic behaviour for $g\to\infty$ were studied for example by Ihara [11], Manin-Valdut [12]. Now, Serre [19], [18] studied the bound for a fixed g and variable q. A part of his results says that for any square $q=p^{2e}$ when $g=1$, and for each square $q\neq 4$ or 9 when $g=2$, there exist curves C_1 and C_2 defined over $\boldsymbol{F}_q$ such that

$$\sharp(C_1(\boldsymbol{F}_q))=1+q+2gp^e\,,\qquad \sharp(C_2(\boldsymbol{F}_q))=1+q-2gp^e\,,$$

that is, there exist curves such that the number of $\boldsymbol{F}_q$-rational points attains Weil's maximum, or minimum. But it remained open, except for several small q and g, whether this is also true for any $g\ge 3$ and for almost all q. (Serre, loc. cit. When q is some power of 2, see also Oort [14].) In this paper, we shall show the following:

THEOREM 1. *For each odd prime p and each positive integer e, there exists a nonsingular irreducible curve C of genus* 3 *defined over $\boldsymbol{F}_p$ such that the number of $\boldsymbol{F}_{p^{2e}}$ rational points attains the maximum* (*resp. the minimum*) *of the Weil inequality for odd* (*resp. even*) *e, that is,*

$$\sharp(C(\boldsymbol{F}_{p^{2e}}))=1+p^{2e}+(-1)^{e+1}6p^e\,.$$

More precisely, there exists a curve C defined over $\boldsymbol{F}_p$ such that the Jacobian variety $J(C)$ of C is isomorphic over $\boldsymbol{F}_{p^2}$ to the product of three copies of a supersingular elliptic curve

* Partly supported by the Grants-in-Aid for Scientific as well as Co-operative Research, The Ministry of Education, Science and Culture, Japan.

1991 *Mathematics Subject Classification.* Primary 11G20; Secondary 14G15, 14G05, 11E41.