Some remarks on the number of rational points of algebraic curves over finite fields

Yasutaka IHARA

To the memory of Takuro Shintani

Let F_q be a finite field with q elements, fixed once and for all. Put

$$A(q)=\lim_{C}\sup\frac{N(C)}{g(C)},$$

where C runs over all complete non-singular absolutely irreducible algebraic curves over F_q with positive genus (counted up to F_q-isomorphisms), $g(C)$ is the genus, and $N(C)$ is the number of F_q-rational points of C. Note that there is only a finite number of non-isomorphic curves over F_q with a given genus. From the Weil's Riemann hypothesis for curves [7] one obtains immediately that $A(q)\leqq 2\sqrt{q}$. The purpose of this note is to point out the following inequalities.

THEOREM (i) $\quad A(q)\leqq\frac{1}{2}\{\sqrt{8q+1}-1\}(<\sqrt{2q}<2\sqrt{q}),$

(ii) *if* $q=p^{2m}$ (p: *a prime*, $m\in\boldsymbol{Z}$), *then* $A(q)\geqq\sqrt{q}-1$.

One may conjecture that $A(q)=\sqrt{q}-1$ when $q=p^{2m}$. We note here that there is an analogous asymptotic estimate of the eigenvalues of Hecke operators, from above, due to Shimura [5].

Note added later. The subject of this paper is closely related to that of Manin [8] contributed also to this volume. Indeed, $A(q)=\mathfrak{S}_q^{-1}$, where $\mathfrak{S}_q$ is as defined in [8] § 5. While Manin points out a very interesting connection with code theory, the main motivation of the present author came from [1] [2] [4]. The relationship between the two papers turned out to be rather of a mutually supplementary nature. For example, our first inequality (i) is giving some answers to the questions raised in [8] § 7, § 9 (a) and our second inequality (ii) and its proof may supplement [8] § 8. The connection with code theory exposed in [8] was essentially new to me.

§ 1. The idea of proof. (i) Let C be with genus g, and

$$\prod_{i=1}^{g}(1-\alpha_i u)(1-\bar{\alpha}_i u)$$

be the numerator of the zeta function of C, $\bar{\alpha}_i$ being the complex conjugate of α_i. For each positive integer $m\geqq 1$, let N_m denote the number of F_{q^m}-rational points of C, so that

$$N_m=q^m+1-\sum_{i=1}^{g}(\alpha_i^m+\bar{\alpha}_i^m)\,;\qquad \alpha_i\bar{\alpha}_i=q\,. \tag{1}$$

If q and m are fixed and g increases, the main term for N_m is the sum of $-(\alpha_i^m+\bar{\alpha}_i^m)$ $(1\leqq i\leqq g)$, and whether N_m is large or small depends on the distribution of arguments of α_i's. The proof of (i) follows immediately from the observation:

$N(C)=N_1$: big$\Rightarrow\arg(\alpha_i)$ are gathered near $\pi\Rightarrow\arg(\alpha_i^2)$ are near $0\Rightarrow N_2$: small, but N_2 cannot be smaller than N_1, contradiction.

(ii) This follows from the theory of uniformization of Shimura curves over finite fields by means of discrete subgroups of $PSL_2(\boldsymbol{R})\times PSL_2(k_{\mathfrak{p}})$ ($\boldsymbol{R}$: the real number field, $k_{\mathfrak{p}}$: a $\mathfrak{p}$-adic field) conjectured by the author [1] and solved (at least) partly by the combination of results due mainly to Shimura, Ihara, Morita.

§2. Proof. (i) Let C, α_i, $\bar{\alpha}_i$ $(1\leqq i\leqq g)$, N_m $(m\geqq 1)$ be as above, and set $a_i=\alpha_i+\bar{\alpha}_i$. Then

$$q+1-\sum_{i=1}^{g}a_i=N_1\leqq N_2=q^2+1+2qg-\sum_{i=1}^{g}a_i^2\,. \tag{2}$$

By (2) and the Schwarz inequality

$$g\cdot\sum_{i=1}^{g}a_i^2\geqq\Big(\sum_{i=1}^{g}a_i\Big)^2,$$

we obtain

$$N_1\leqq q^2+1+2qg-g^{-1}\cdot(N_1-q-1)^2\,,$$

or equivalently,

$$N_1^2-(2q+2-g)N_1+(q+1)^2-(q^2+1)g-2qg^2\leqq 0\,.$$

Therefore,

$$2N_1\leqq\sqrt{(8q+1)g^2+(4q^2-4q)g}-(g-2q-2)$$

which implies

$$\limsup\frac{N_1}{g}\leqq\frac{1}{2}\{\sqrt{8q+1}-1\}\,.$$

(If we use $N_2\geqq 0$ instead of $N_2\geqq N_1$ in (2), we obtain $A(q)\leqq\sqrt{2q}$ which is slightly weaker than the above but stronger than the direct consequence $A(q)\leqq 2\sqrt{q}$ of (1) for $m=1$.)

(ii) *The case* $m=1$. Let n be a positive integer with $n\not\equiv 0 \pmod p$, and C_n be the *p-canonical modular curve of level n over* F_{p^2}, i.e., a complete non-singular curve over F_{p^2} whose function field is the field K_n defined in [2]. Let $\mathfrak{S}_n$ be the set of all points of C_n which parametrize *supersingular* elliptic curves. A characteristic property of this p-canonical model is that all points of $\mathfrak{S}_n$ are F_{p^2}-rational [1] [2]. Put

$$d_n=[K_n : K_1]=(SL_2(\boldsymbol{Z}/n) : \{\pm I\}).$$

If $n>1$, the genus g_n of C_n and the cardinality h_n of $\mathfrak{S}_n$ are given by the formulae

$$g_n-1=\frac{d_n(n-6)}{12n},$$

$$h_n=\frac{d_n}{12}(p-1).$$

Therefore,

$$A(p^2)\geqq\limsup_{n\to\infty}\frac{p-1}{1-6n^{-1}+12d_n^{-1}}=p-1.$$

The general case. We use similar results on Shimura curves. Let $k_{\mathfrak{p}}$ be a $\mathfrak{p}$-adic field with $N(\mathfrak{p})=p^m$, and Γ be an arithmetically defined discrete subgroup of $PSL_2(\boldsymbol{R})\times PSL_2(k_{\mathfrak{p}})$ which corresponds with a congruence relation in the sense of [3] (§ 6). There are many such examples due to [6] (for 'almost all $\mathfrak{p}$'), [4] (for individual $\mathfrak{p}$). On the other hand, it is shown [3] that each such Γ gives rise to a pair $(C, \mathfrak{S})$ of a curve C over $F_{p^{2m}}$ and a set $\mathfrak{S}$ of (not necessarily all) $F_{p^{2m}}$-rational points of C, called special points, in a functorial manner. Since $|\mathfrak{S}|\geqq(p^m-1)(g-1)$ ([3] § 1), g being the genus of C, and since $g\to\infty$ as we pass to subgroups of Γ with large finite indices, we obtain $A(p^{2m})\geqq p^m-1$.

q. e. d.

REMARK. The modular curves C_n treated separately in the proof of the case $m=1$ correspond to $\Gamma=PSL_2\left(\boldsymbol{Z}\left[\frac{1}{p}\right]\right)$ and its principal congruence subgroups of level n.

References

[1] Ihara, Y., (a) The congruence monodromy problems, J. Math. Soc. Japan **20** (1968), 107-121.
(b) On congruence monodromy problems, Lecture Notes, Univ. Tokyo, I (1968), II (1969).

[2] Ihara, Y., On modular curves over finite fields, Proc. Intern. Colloq. on Discrete subgroups of Lie groups and applications to moduli, Bombay 1973, Oxford Univ.

Press, 161-202.
[3] Ihara, Y., Congruence relations and Shimura curves, I, Proc. Symp. in pure Math. Vol. 33, Part 2, Amer. Math. Soc., 1979, 291-311; II, J. Fac. Sci., Univ. Tokyo, Sect. IA **25** (1979), 301-361.
[4] Morita, Y., Reduction mod $\mathfrak{P}$ of Shimura curves, Hokkaido Math. J. **10** (1981), 209-238.
[5] Shimura, G., Moduli of abelian varieties and number theory, Proc. Symp. in Pure Math. Vol. 9, Amer. Math. Soc., 1966, 312-332.
[6] Shimura, G., On canonical models of arithmetic quotients of bounded symmetric domains I, Ann. of Math. **91** (1970), 144-222; II, ibid **92** (1970), 528-549.
[7] Weil, A., Courbes algébriques et variétés abéliennes, Hermann.
[8] Manin, Yu. I., What is the maximum number of points on a curve over $\boldsymbol{F}_2$?, in this volume; i.e., J. Fac. Sci., Univ. Tokyo, Sect. IA 28 (1981), 715-720.

(Received June 10, 1981)

Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo
113 Japan