

SUPERSINGULAR j -INVARIANTS AS SINGULAR MODULI MOD p

MASANOBU KANEKO¹

(Received April 11, 1989)

1. Introduction. In this paper we shall give some results concerned with the reduction modulo p of the minimal polynomials of “singular moduli”. Let $O_D = \mathbf{Z} \left[\frac{1}{2}(D + \sqrt{-D}) \right]$ be the imaginary quadratic order of discriminant $-D$ ($D \equiv 0, 3 \pmod{4}$). We denote by $P_D(X)$ the monic polynomial whose roots are precisely the distinct j -invariants of elliptic curves over $\bar{\mathbf{Q}}$ with complex multiplication by O_D ($\bar{\mathbf{Q}}$ is the algebraic closure of the rationals \mathbf{Q}). It is well known that $P_D(X)$ has its coefficients in the ring of integers \mathbf{Z} and the degree of $P_D(X)$ is equal to the class number of O_D . Let E be an elliptic curve defined over \mathbf{Q} and $J = j(E)$ be its j -invariant. As was observed by N. Elkies in [5], if a prime factor p of the numerator of $P_D(J)$ satisfies $\left(\frac{\mathbf{Q}(\sqrt{-D})}{p} \right) \neq 1$ (i.e., p does not split completely in $\mathbf{Q}(\sqrt{-D})$), then (provided that E has good reduction at p) p is supersingular for E . Conversely, every supersingular prime p for E appears as a prime factor of the numerator of $P_D(J)$ for some D with $\left(\frac{\mathbf{Q}(\sqrt{-D})}{p} \right) \neq 1$. Elkies pointed out that, for supersingular p , such D can always be found within the bound $D < 2p^{2/3}$. Furthermore he made an observation that such bound seemed to be in no way best possible. The first purpose of this paper is to give a better bound $D \leq \frac{4}{\sqrt{3}}\sqrt{p}$, which is a consequence of the following

Theorem 1. *Every supersingular j -invariant contained in the prime field \mathbf{F}_p is a root of some $P_D(X) \pmod{p}$ with $D \leq \frac{4}{\sqrt{3}}\sqrt{p}$.*

Here we recall that supersingular j -invariants in characteristic p are all contained in \mathbf{F}_{p^2} (the field with p^2 elements) and some of them are in \mathbf{F}_p whose cardinality is related to the class number of the field $\mathbf{Q}(\sqrt{-p})$. As our E is defined over \mathbf{Q} , $j(E) \pmod{p}$ is contained in \mathbf{F}_p .

¹ This work was supported by Grant-in-Aid for Scientific Research, The Ministry of Education, Science and Culture.

Our next theorem concerns common roots of two polynomials $P_{D_1}(X) \pmod p$ and $P_{D_2}(X) \pmod p$.

Theorem 2. *If two different discriminants $-D_1$ and $-D_2$ satisfy $D_1 D_2 < 4p$ (in particular $D_1, D_2 < 2\sqrt{p}$), then two polynomials $P_{D_1}(X) \pmod p$ and $P_{D_2}(X) \pmod p$ in $\mathbf{F}_p[X]$ have no roots in common. In other words, every prime factor p of the resultant of $P_{D_1}(X)$ and $P_{D_2}(X)$ satisfies $p \leq \frac{D_1 D_2}{4}$.*

Furthermore, if $\mathbf{Q}(\sqrt{-D_1}) = \mathbf{Q}(\sqrt{-D_2})$, the above inequality $D_1 D_2 < 4p$ (resp. $p \leq \frac{D_1 D_2}{4}$) can be replaced by $D_1 D_2 < p^2$ (resp. $p \leq \sqrt{D_1 D_2}$).

As our proof will show, each prime factor p of the resultant of $P_{D_1}(X)$ and $P_{D_2}(X)$ divides a positive integer of the form $(D_1 D_2 - x^2)/4$. When D_1 and D_2 are fundamental discriminants and relatively prime, this fact was given by B. Gross and D. Zagier in [6] as a corollary of their explicit prime factorization of the resultant of $P_{D_1}(X)$ and $P_{D_2}(X)$.

By Deuring’s theory of reduction of elliptic curves, Theorem 2 can be reformulated as the following Theorem 2’ which is a little more general than a theorem of Eichler [3] but the proof is essentially the same. Let $\mathbf{Q}_{\infty, p}$ be the definite quaternion algebra over \mathbf{Q} which ramifies only at p . The order O_D is said to be optimally embedded in a maximal order R of $\mathbf{Q}_{\infty, p}$ if $\mathbf{Q}(\sqrt{-D})$ embeds into $\mathbf{Q}_{\infty, p}$ and $R \cap \mathbf{Q}(\sqrt{-D}) = O_D$.

Theorem 2’. *Suppose that two quadratic orders O_{D_1} and O_{D_2} are optimally embedded in a maximal order of $\mathbf{Q}_{\infty, p}$ with different images, then the inequality $D_1 D_2 \geq 4p$ holds. If $\mathbf{Q}(\sqrt{-D_1}) = \mathbf{Q}(\sqrt{-D_2})$, this inequality can be replaced by $D_1 D_2 \geq p^2$.*

In the appendix, we shall give an alternative proof of a proposition by Elkies [5] which was crucial for his proof of the infinitude of supersingular primes for elliptic curves over \mathbf{Q} .

The author is very grateful to Professor T. Ibukiyama for his helpful communications. The constant of our Theorem 1 was improved to the present form by his remark.

2. Proof of Theorem 1. Let E be an arbitrary supersingular elliptic curve defined over \mathbf{F}_p (hence its j -invariant is contained in \mathbf{F}_p) and $\text{End } E$ its endomorphism ring over the algebraic closure of \mathbf{F}_p . To prove Theorem 1, it suffices to show that $\text{End } E$ contains an order O_D with $D \leq \frac{4}{\sqrt{3}} \sqrt{p}$. For, if an order O_D is contained in $\text{End } E$, by Deuring’s Lifting Lemma ([2, p. 259]), there exists an elliptic curve over $\bar{\mathbf{Q}}$ with complex multiplication by some order $O_{D'}$

containing O_D whose reduction to characteristic p is isomorphic to E . Then the j -invariant of E is a root of $P_{D'}(X) \pmod p$ with $D' \leq D \leq \frac{4}{\sqrt{3}}\sqrt{p}$ and Theorem 1 follows. It is well known that, when E is defined over \mathbf{F}_p , $\text{End } E$ is isomorphic to a maximal order of $\mathbf{Q}_{\infty,p}$ which contains an element with the minimal polynomial X^2+p (Frobenius element). On the other hand, such a maximal order has been described explicitly by Ibukiyama in [7] as follows. Choose a prime q such that $q \equiv 3 \pmod 8$ and $\left(\frac{-p}{q}\right) = 1$. Here, $\left(\frac{-p}{q}\right)$ is the Legendre's symbol. Then $\mathbf{Q}_{\infty,p}$ can be realized as

$$\mathbf{Q}_{\infty,p} = \mathbf{Q} + \mathbf{Q}\alpha + \mathbf{Q}\beta + \mathbf{Q}\alpha\beta,$$

where $\alpha^2 = -p$, $\beta^2 = -q$, and $\alpha\beta = -\beta\alpha$. Choosing an integer r such that $r^2 + p \equiv 0 \pmod q$, put

$$O(q, r) = \mathbf{Z} + \mathbf{Z}\frac{1+\beta}{2} + \mathbf{Z}\frac{\alpha(1+\beta)}{2} + \mathbf{Z}\frac{(r+\alpha)\beta}{q}.$$

When $p \equiv 3 \pmod 4$, we further choose an integer r' such that $r'^2 + p \equiv 0 \pmod{4q}$ and put

$$O'(q, r') = \mathbf{Z} + \mathbf{Z}\frac{1+\alpha}{2} + \mathbf{Z}\beta + \mathbf{Z}\frac{(r'+\alpha)\beta}{2q}.$$

Then a part of Ibukiyama's results says that both $O(q, r)$ and $O'(q, r')$ (their isomorphism classes depend only on q not on r nor r') are maximal orders of $\mathbf{Q}_{\infty,p}$ and any maximal order which contains an element with the minimal polynomial X^2+p is isomorphic to $O(q, r)$ or $O'(q, r')$ with suitable choice of q . Therefore our task is to show that for any q both $O(q, r)$ and $O'(q, r')$ contain an element $\frac{1}{2}(D + \sqrt{-D})$ (i.e., an element with the minimal polynomial $X^2 - DX + \frac{1}{4}(D^2 + D)$) with $D \leq \frac{4}{\sqrt{3}}\sqrt{p}$.

We start with $O(q, r)$. Let

$$\gamma = w + x\frac{1+\beta}{2} + y\frac{\alpha(1+\beta)}{2} + z\frac{(r+\alpha)\beta}{q}$$

denote an element in $O(q, r)$ ($w, x, y, z \in \mathbf{Z}$) and consider the following diophantine equations:

$$tr(\gamma) = 2w + x = D$$

and

$$n(\gamma) = \left(w + \frac{x}{2}\right)^2 + \frac{p}{4}y^2 + q\left(\frac{x}{2} + \frac{zr}{q}\right)^2 + pq\left(\frac{y}{2} + \frac{z}{q}\right)^2 = \frac{D^2 + D}{4},$$

where $tr(\gamma)$ (resp. $n(\gamma)$) is the reduced trace (resp. norm) of γ . These equations are equivalent to

$$(2-1) \quad 2w+x = D,$$

$$(2-2) \quad py^2+q\left(x+\frac{2zr}{q}\right)^2+pq\left(y+\frac{2z}{q}\right)^2 = D.$$

Note that, by our choice of q and r , for any x, y, z in \mathbf{Z} the left hand side of (2-2) always represent an integer congruent modulo 2 to x . So, if integers x, y and z satisfies (2-2), we can always find an integer w which satisfies (2-1). Therefore, the problem is to find such D not greater than $\frac{4}{\sqrt{3}}\sqrt{p}$ that the equation (2-2) is soluble. Now, if we put $y=0$ in (2-2), we have

$$(2-3) \quad \frac{(qx+2zr)^2+4pz^2}{q} = D$$

and the left hand side of (2-3) is a positive definite binary quadratic form in x and z with determinant $4p$. Hence a classical theorem (cf. e.g. [1, p. 30]) assures that there exists integers x and z so that the left hand side of (2-3) is less than or equal to $\sqrt{\frac{4 \times 4p}{3}} = \frac{4}{\sqrt{3}}\sqrt{p}$. This proves our assertion.

As for $O'(q, r')$ (when $p \equiv 3 \pmod{4}$), the same calculations will do. Put

$$\gamma = w+x\frac{1+\alpha}{2}+y\beta+z\frac{(r'+\alpha)\beta}{2q} \in O'(q, r').$$

From the conditions $tr(\gamma)=D$ and $n(\gamma)=\frac{D^2+D}{4}$ we have

$$(2-4) \quad 2w+x = D$$

$$(2-5) \quad px^2+q\left(2y+\frac{zr'}{q}\right)^2+\frac{pz^2}{q} = D.$$

As before, for any x, y, z in \mathbf{Z} the left hand side of (2-5) is an integer congruent modulo 2 to x and hence the w determined by (2-4) is in \mathbf{Z} . Again by putting $x=0$ the left hand side of (2-5) is a positive definite binary quadratic form of determinant $4p$. Therefore there exists an element $\gamma \in O'(q, r')$ whose minimal polynomial is $X^2-DX+\frac{1}{4}(D^2+D)$ with $D \leq \frac{4}{\sqrt{3}}\sqrt{p}$. This concludes our proof of Theorem 1.

3. Proof of Theorem 2'. Suppose that O_{D_1} and O_{D_2} are optimally embedded in a maximal order R of $\mathbf{Q}_{\infty, p}$ with different images. Let α_i ($i=1, 2$) be the images of $\frac{1}{2}(D_i+\sqrt{-D_i})$ by these embeddings ($\alpha_1 \neq \alpha_2$). In R , consider the \mathbf{Z} -module L generated by $1, \alpha_1, \alpha_2$, and $\alpha_1\alpha_2$. In general, a module $\mathbf{Z}\mu_1+$

$\mathbf{Z}\mu_2 + \mathbf{Z}\mu_3 + \mathbf{Z}\mu_4$ in $\mathcal{Q}_{\infty,p}$ has rank 4 if and only if its discriminant $D(\mu_1, \mu_2, \mu_3, \mu_4) = \det(\text{tr}(\mu_i \mu_j))$ is not equal to 0 (cf. e.g. [3, Ch. 1 §2 Th. 1]). As for our L we have by a direct calculation

$$D(1, \alpha_1, \alpha_2, \alpha_1 \alpha_2) = - \left\{ \frac{D_1 D_2 - (2s - D_1 D_2)^2}{4} \right\}^2,$$

where $s = \text{tr}(\alpha_1 \alpha_2) (\in \mathbf{Z})$. Now consider the element $\beta = \left(\alpha_1 - \frac{D_1}{2}\right) \left(\alpha_2 - \frac{D_2}{2}\right)$ in R . It does not belong to \mathcal{Q} (the center of $\mathcal{Q}_{\infty,p}$) even when $\mathcal{Q}(\sqrt{-D_1}) = \mathcal{Q}(\sqrt{-D_2})$ because of our assumption that O_{D_1} and O_{D_2} are optimally embedded with different images. Hence

$$\begin{aligned} \text{tr}(\beta)^2 - 4n(\beta) &= \left(s - \frac{D_1 D_2}{2}\right)^2 - 4 \times \frac{D_1 D_2}{16} \\ &= \frac{(2s - D_1 D_2)^2 - D_1 D_2}{4} < 0. \end{aligned}$$

Therefore, we have $D(1, \alpha_1, \alpha_1, \alpha_1 \alpha_2) \neq 0$. On the other hand, we can readily show that L is a subring ($\alpha_i^2, \alpha_2 \alpha_1 \in L$ etc.) of R . Hence we conclude that L is an order of $\mathcal{Q}_{\infty,p}$. As the discriminant of an order in $\mathcal{Q}_{\infty,p}$ is divisible by p^2 (the discriminant of maximal orders), we conclude that p divides the positive integer $\frac{1}{4}(D_1 D_2 - (2s - D_1 D_2)^2)$, in particular $p \leq \frac{D_1 D_2}{4}$.

When D_1 and D_2 are given as $D_1 = f_1^2 D$ and $D_2 = f_2^2 D$ with positive integers f_1, f_2, D , we have

$$\frac{D_1 D_2 - (2s - D_1 D_2)^2}{4} = \frac{(f_1 f_2 D - (2s - D_1 D_2))(f_1 f_2 D + (2s - D_1 D_2))}{4} (> 0).$$

As the inequality $|f_1 f_2 D \pm (2s - D_1 D_2)| \leq 2f_1 f_2 D$ holds and both $f_1 f_2 D - (2s - D_1 D_2)$ and $f_1 f_2 D + (2s - D_1 D_2)$ are even numbers (since they have same parity and their product is divisible by 4), we must have $p \leq f_1 f_2 D = \sqrt{D_1 D_2}$. This completes our proof.

Appendix. An alternative proof of a proposition in [5]². Let p be a prime number. Recall that $P_D(X)$ denotes the minimal polynomial of a singular modulus having O_D as complex multiplication. In [5] the following proposition played an essential role.

Proposition (Elkies). *Assume $p \equiv 3 \pmod{4}$. We have*

$$\begin{aligned} P_p(X) &\equiv (X - 12^3) (R(X))^2 \pmod{p} \\ P_{4p}(X) &\equiv (X - 12^3) (S(X))^2 \pmod{p} \end{aligned}$$

2 N. Elkies informed the author that the following proof had also been discovered by D. Zagier.

with some polynomials $R(X), S(X) \in \mathbf{Z}[X]$.

We shall give a proof of this proposition by using two classical results due to Kronecker. First we shall prove the following Proposition'. (Actually in this form Elkies used the proposition.)

Proposition'. *We have*

$$\begin{aligned} P_p(X) &\equiv (T(X))^2 \pmod{p} \quad \text{if } p \equiv 1 \pmod{4}, \\ P_p(X) P_{4p}(X) &\equiv (U(X))^2 \pmod{p} \quad \text{if } p \equiv 3 \pmod{4} \end{aligned}$$

with some polynomials $T(X), U(X) \in \mathbf{Z}[X]$.

Proof. Let $\Phi_p(X, Y)$ denote the p -th modular polynomial. (cf. [8, Ch. 5 §2]) The following two properties on $\Phi_p(X, Y)$ are known as the "Kronecker's relations":

$$(4-1) \quad \Phi_p(X, Y) \equiv (X^p - Y)(X - Y^p) \pmod{p},$$

$$(4-2) \quad \begin{aligned} \Phi_p(X, X) &= -\prod_D P_D(X)^{r(D)} \\ &= \begin{cases} -P_{4p}(X) \prod_{p \nmid D} P_D(X)^2 & \text{if } p \equiv 1 \pmod{4} \\ -P_p(X) P_{4p}(X) \prod_{p \nmid D} P_D(X)^2 & \text{if } p \equiv 3 \pmod{4}, \end{cases} \end{aligned}$$

where the product runs over such D that the order O_D contains an element of norm p and $r(D)=1$ or 2 according as $p|D$ or $p \nmid D$ (cf. [8, Ch. 5 §2 and Ch. 10 App.]) By putting $Y=X$ in (4-1) we get

$$(4-3) \quad \Phi_p(X, X) \equiv -(X^p - X)^2 \pmod{p}.$$

Proposition' follows immediately from this and (4-2).

Proof of Proposition. The above relations (4-2) and (4-3) shows that, modulo p , the polynomial $P_p(X) P_{4p}(X)$ is a square and divides $(X^p - X)^2$. Hence each of its roots has multiplicity 2. By Lemma 1 in [5], both $P_p(X) \pmod{p}$ and $P_{4p}(X) \pmod{p}$ have 12^3 as one of their roots. On the other hand, a lemma of Ibukiyama ([7, Lem. 1.8]) implies that there are no other common roots of $P_p(X) \pmod{p}$ and $P_{4p}(X) \pmod{p}$. Therefore the conclusion follows.

References

- [1] J.W.S. Cassels: "An Introduction to the Geometry of Numbers," Springer, 1959.
- [2] M. Deuring: *Die Typen der Multiplikatorenringe elliptischer Funktionen Körper*, Abh. Math. Sem. Univ. Hamburg **14** (1941), 197-272.
- [3] M. Eichler: "Lectures on Modular Correspondences," Tata Inst. Fundamental

- Res., Bombay, 1955/6.
- [4] M. Eichler: *New formulas for the class number of imaginary quadratic fields*, Acta Arith. **49** (1987), 35–43.
 - [5] N.D. Elkies: *The existence of infinitely many supersingular primes for every elliptic curve over \mathbf{Q}* , Invent. Math. **89** (1987), 561–567.
 - [6] B.H. Gross and D. Zagier: *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220.
 - [7] T. Ibukiyama: *On maximal orders of division quaternion algebra over the rational number field with certain optimal embeddings*, Nagoya Math. J. **88** (1982), 181–195.
 - [8] S. Lang: “*Elliptic Functions*, Second Edition,” Springer, 1987.

Department of Mathematics
Osaka University,
Toyonaka, Osaka 560
Japan

