

A Note on Elkies' Proof

STEPHEN J.M. MILDENHALL

March, 1991

Abstract. We give a "classical" proof of a proposition, used by Elkies to prove that an elliptic curve defined over \mathbb{Q} has infinitely many primes of supersingular reduction.

Let \mathcal{O}_d be the quadratic order of discriminant d . Recall that $j(\mathcal{O}_d)$ is an algebraic integer, [2, Theorem 11.1], and let $P_d(X) \in \mathbb{Z}[X]$ be its minimal polynomial.

Pick a rational prime $l \geq 5$. Let X be the set of elliptic curves defined over \mathbb{F}_l , up to isomorphism over \mathbb{F}_l . We can write $X = X^{ss} \amalg X^{ord}$ as a disjoint union of supersingular and ordinary elliptic curves.

Define a "polynomial" (after [3]) by

$$f_d(X) = \prod_{f^2 | d} P_{d/f^2}(X)^{w(d/f^2)}$$

where the product is over all $f^2 | d$ such that d/f^2 is a discriminant, and $w(d) = 2/|\mathcal{O}_d^\times|$. We have

$$f_{4l}(X) = \begin{cases} P_{-4l}(X) & l \equiv 1 \pmod{4} \\ P_{-l}(X)P_{-4l}(X) & l \equiv 3 \pmod{4}. \end{cases}$$

Our main result is

PROPOSITION. *Let $l \geq 5$ be a rational prime. Then*

$$f_{4l}(X) \equiv \prod_{\substack{j \in \mathbb{F}_l \\ j \text{ supersingular}}} (X - j)^2 \pmod{l},$$

is a square mod l .

Before giving the proof, we recall how Elkies uses this result to prove

THEOREM. [1, Theorem 1] *Let E be an elliptic curve defined over \mathbb{Q} . Then E has infinitely many primes of supersingular reduction.*

PROOF: Let $J = j(E)$. If $l \equiv 3 \pmod{4}$ is prime, then, from the q -expansion for j , it is easy to see that the real root of $P_{-l}(X)$ tends to $-\infty$ and that the real root of $P_{-4l}(X)$ tends to ∞ as l tend to ∞ . Therefore, for fixed J , $P_{-l}(J)P_{-4l}(J) < 0$ if l is large enough, say $l \geq L_J$.

Suppose p_1, \dots, p_r is a list of supersingular primes for E . Pick a prime $l \equiv 3 \pmod{4}$ so that $(p_i/l) = 1$ for $i = 1, \dots, r$ and so that $l \geq L_J$. Then, there is a supersingular prime in the numerator of $P_{-l}(J)P_{-4l}(J)$. Otherwise, the numerator

of $P_{-l}(J)P_{-4l}(J)$ would be a product of ordinary primes. Hence $P_{-l}(J)P_{-4l}(J)$ would be a product of quadratic residues modulo l , and therefore a square mod l . (Notice that $(-l/p_i) = (p_i/l)$, by quadratic reciprocity.) Both $P_{-l}(X)$ and $P_{-4l}(X)$ have odd degree (by the theory of genera) and so the denominator of $P_{-l}(J)P_{-4l}(J)$ is a square. Therefore we have

$$P_{-l}(J)P_{-4l}(J) = - \left(\frac{\text{square mod } l}{\text{square}} \right).$$

This is a contradiction, because $P_{-l}(J)P_{-4l}(J)$ is a square mod l by our proposition, but $(-1/l) = -1$.

Therefore there is a supersingular prime, p , dividing the numerator of $P_{-l}(J)P_{-4l}(J)$. Since $(-l/p) = 0$ or -1 , p cannot be one of the p_i ! ■

PROOF OF PROPOSITION: If E is an elliptic curve, let $w(E) = 2/|Aut_{\overline{\mathbb{F}_l}}(E)|$. Notice that if E has complex multiplication by \mathcal{O}_d , then $w(E) = w(d)$.

The $\overline{\mathbb{F}_l}$ -isomorphism class of $E \in X$ splits into $|Aut_{\overline{\mathbb{F}_l}}(E)|$ different \mathbb{F}_l -isomorphism classes. Therefore

$$\begin{aligned} \prod_{\substack{j \in \mathbb{F}_l \\ j \text{ singular}}} (X - j)^2 &= \prod_{E \in X^{ord}} (X - j(E))^{w(E)} \\ &\equiv \prod_{\substack{0 \neq a \in \mathbb{Z} \\ a^2 - 4l < 0}} f_{a^2 - 4l}(X) \pmod{l}. \end{aligned} \quad (1)$$

(E is supersingular in characteristic $l \geq 5$ if and only if the trace of l -Frobenius $= 0$.) Let $\Phi_m(X, Y)$ be the modular equation of level m . We have Kronecker's congruence, [2, Theorem 11.18],

$$\Phi_l(X, Y) \equiv (X^l - Y)(X - Y^l) \pmod{l},$$

and therefore

$$\Phi_l(X, X) \equiv -(X^l - X)^2 \equiv - \prod_{j=0}^{l-1} (X - j)^2 \pmod{l}. \quad (2)$$

On the other hand, we have Kronecker's identity, [3, (4.3)],

$$\begin{aligned} \Phi_l(X, X) &= \pm \prod_{\substack{a \in \mathbb{Z} \\ a^2 - 4l < 0}} f_{a^2 - 4l}(X) \\ &= \pm f_{4l}(X) \prod_{\substack{0 \neq a \in \mathbb{Z} \\ a^2 - 4l < 0}} f_{a^2 - 4l}(X) \\ &\equiv \pm f_{4l}(X) \prod_{\substack{j \in \mathbb{F}_l \\ j \text{ singular}}} (X - j)^2 \end{aligned} \quad (3)$$

by (1). Combining (2) and (3) we get

$$\prod_{j=0}^{l-1} (X-j)^2 \equiv f_{4l}(X) \prod_{\substack{j \in \mathbf{F}_l \\ j \text{ singular}}} (X-j)^2,$$

where the leading coefficient determines the sign. The result follows because $\mathbf{F}_l[X]$ is a unique factorization domain. ■

The proposition shows that the number of supersingular curves defined over \mathbf{F}_l is

$$\begin{cases} h(\mathcal{O}_{-4l})/2 & l \equiv 1 \pmod{4} \\ h(\mathcal{O}_{-l}) & l \equiv 7 \pmod{8} \\ 2h(\mathcal{O}_{-l}) & l \equiv 3 \pmod{8}, \end{cases}$$

which is a special case of the Eichler trace formula.

We end with some examples. If $l = 5$ then, modulo 5

$$\begin{aligned} \Phi_5(X, X) &\equiv P_{-20}(X) \cdot (P_{-4}(X)P_{-11}(X)P_{-16}(X)P_{-19}(X))^2 \\ &\equiv X^2 \cdot ((X+2)(X+3)(X+4)(X+1))^2. \end{aligned}$$

If $l = 7$ then, modulo 7

$$\begin{aligned} \Phi_7(X, X) &\equiv P_{-7}(X)P_{-28}(X) \cdot (P_{-3}(X)P_{-12}(X)P_{-19}(X)P_{-24}(X)P_{-27}(X))^2 \\ &\equiv (X+1)(X+1) \cdot (X(X+5)(X+6)((X+2)(X+3))(X+4))^2. \end{aligned}$$

If $l = 71$ then

$$\begin{aligned} P_{-71}(X)P_{-284}(X) &\equiv (23+X)^2(31+X)^2(47+X)(54+X)^2 \\ &\quad X^2(5+X)^2(30+X)^2(47+X) \pmod{71}, \end{aligned}$$

and we see all the supersingular invariants in characteristic 71 are defined over \mathbf{F}_{71} . Finally, if $l = 389$,

$$\begin{aligned} P_{-1556}(X) &\equiv X^2(31+X)^2(62+X)^2(71+X)^2(169+X)^2(235+X)^2(268+X)^2 \\ &\quad (353+X)^2(372+X)^2(373+X)^2(382+X)^2 \pmod{389}. \end{aligned}$$

I would like to thank David Roberts for his help in writing this paper. The same proof has been found independently by Zagier and by Kaneko.

REFERENCES

- (1) N.D.ELKIES, The existence of infinitely many supersingular primes for every elliptic curve over \mathbf{Q} , *Invent. Math.* **89** (1987), 561–567.
- (2) D.A.COX, “Primes of the Form $x^2 + ny^2$,” Wiley–Interscience, New York, 1989.
- (3) B.GROSS AND D.ZAGIER, On Singular Moduli, *J. Reine Angew. Math.* **355** (1985) 191–220.