COMPOSITIO MATHEMATICA

GERHARD FREY

A remark about isogenies of elliptic curves over quadratic fields

Compositio Mathematica, tome 58, n° 1 (1986), p. 133-134

<http://www.numdam.org/item?id=CM_1986__58_1_133_0>

[1] Compositio Mathematica 58 (1986) 133–134

A REMARK ABOUT ISOGENIES OF ELLIPTIC CURVES OVER QUADRATIC FIELDS

Gerhard Frey

We want to prove the following

THEOREM: *Let p be a prime > 240. Then there are only finitely many elements $j \in \overline{\mathbb{Q}}$ with $[\mathbb{Q}(j): \mathbb{Q}] \leqslant 2$ such that there is an elliptic curve E with j-invariant equal to j having an isogeny of degree p rational over a quadratic extension of $\mathbb{Q}$.*

At first we introduce some notation:

Let $X_0(p)$ be the modular curve parametrizing elliptic curves with isogenies of degree p, its Jacobian is denoted by $J_0(p)$ and its Eisenstein quotient by J (cf. [Ma]). Let π be the quotient mapping from $J_0(p)$ to J.

The first ingredient we use is

Fact 1 (Mazur): $J(\mathbb{Q})$ is finite.

Secondly we use

Fact 2 (essentially due to Ogg): Assume that $K|\mathbb{Q}$ is an extension such that the residue field of K with respect to a place $\mathfrak{q}|2$ is contained in $\mathbb{F}_4$. Then for $p > 240$ there is no non constant function f on $X_0(p)$ rational over K whose pole divisor has a degree $\leqslant 4$.

We indicate shortly how fact 2 follows: Let D be the pole divisor of f. Extend D to a divisor $\mathscr{D}$ of the minimal model $\mathscr{X}_0(p)$ of X_0 with respect to $\mathfrak{q}$ over $O_{\mathfrak{q}}$ (the ring of integers with respect to $\mathfrak{q}$). Then $H^0(\mathscr{X}_0(p) \times \mathbb{F}_4, \mathscr{O}(\mathscr{D} \times \mathbb{F}_4))$ is of dimension > 1 and hence there is a mapping $f_{\mathfrak{q}}$: $\mathscr{X}_0(p) \times \mathbb{F}_4 \to \mathbb{P}^1|_{\mathbb{F}_4}$ of degree $\leqslant 4$. Hence $\#\mathscr{X}_0(p)(\mathbb{F}_4) \leqslant 20$. But due to [Ogg] one knows that $\mathscr{X}_0(p) \times \mathbb{F}_4$ has at least $[p/12] + 1$ $\mathbb{F}_4$-rational points.

The third essential result is the celebrated theorem of Faltings:

Fact 3: Let Γ be a scheme of finite type of dimension $\leqslant 1$ defined over a finite number field K such that the set of K-rational points $\Gamma(K)$ is infinite. Then $\Gamma \times \overline{\mathbb{Q}}$ contains a curve of genus 0 or genus 1.

Now we come to the

PROOF OF THE THEOREM:

(1) Let $X_0 p)^{(2)}$ denote the symmetric product of $X_0(p)$ with itself: $X_0(p)^{(2)} = (X_0(p) \times X_0(p))/\mathfrak{S}_2$ where $\mathfrak{S}$ operates by interchanging the components.

Hence the points of $X_0(p)^{(2)}$ correspond to sets $\overline{(x, y)} :=$

$\{(x, y), (y, x)\}$ with $(x, y) \in X_0(p) \times X_0(p)$. We have a mapping

$$\varphi\colon X_0(p)^{(2)} \to J$$

by sending $\overline{(x, y)}$ to $\pi(((x)+(y)-2(\infty)))$ where as usual ∞ is the cusp corresponding to $i \cdot \infty$ on the upper half plane and $((x)+(y)-2(\infty))$ is the divisor class of the divisor $(x)+(y)-2(\infty)$.

$\Gamma := \varphi^{-1}(J(\mathbb{Q}))$ is a $\mathbb{Q}$-rational subscheme of $X_0(p)^{(2)}$ of dimension $\leqslant 1$. For otherwise the image of $X_0(p)^{(2)}$ under φ would be zero dimensional and connected. But $\varphi(\overline{(\infty, 0)}) = \pi((0)-(\infty))$ is different from $\varphi(\overline{(\infty, \infty)})$ being the zero element of J.

(ii) Now assume that E is an elliptic curve defined over a quadratic field K_E with a K_E-rational isogeny of degree p. Let x be the corresponding point in $X_0(p)(K_E)$ and let σ be the involution of $K_E/\mathbb{Q}$. Then $\overline{(x, \sigma x)} \in X_0(p)^{(2)}(\mathbb{Q})$ and since $(x-(\infty)+\sigma x-(\infty)) \in J_0(p)(\mathbb{Q})$ we have: $\overline{(x, \sigma x)} \in \Gamma(\mathbb{Q})$.

Now assume that there are infinitely many different points on $X_0(p)(\overline{\mathbb{Q}})$ obtained in this manner. Then fact 3 implies that there is a curve C in $\Gamma \times \overline{\mathbb{Q}}$ having genus $\leqslant 1$. Now let $C = C_1, \ldots, C_n$ be all the conjugates of C over $\mathbb{Q}$ and let τ be an automorphism of $\overline{\mathbb{Q}}$ mapping C to C_i. If $P \in C_1(\overline{\mathbb{Q}}) \cap \Gamma(\mathbb{Q})$ then $P = \tau P \in C_i(\overline{\mathbb{Q}})$. Since we can assume that we have infinitely many points in $C_1(\overline{\mathbb{Q}}) \cap \Gamma(\mathbb{Q})$ we get that C is already defined over $\mathbb{Q}$ and that $\Gamma(\mathbb{Q}) \cap C(\overline{\mathbb{Q}}) = C(\mathbb{Q})$. Let C_1 be the preimage of C in $X_0(p) \times X_0(p)$ and (without loss of generality) $p_1(C_1) = X_0(p)$ where p_1 is the projection of $X_0(p) \times X_0(p)$ to the first component. The degree of C_1 over C is equal to 2.

Now choose a point $P = \overline{(x, y)} \in C(\mathbb{Q})$ and a $\mathbb{Q}$-rational function z on C with pole divisor equal to $(g(C)+1)(P)$ such that z has a zero in a point $Q \in C(\mathbb{Q})$ with $Q = \overline{(x_1, y_1)}$ and $x_1 \neq x$. Then z induces a $\mathbb{Q}$-rational function z_1 on C_1 whose norm with respect to p_1 is non constant $\mathbb{Q}$-rational with pole divisor of degree $\leqslant 4$.

But this contradicts fact 2, and hence the theorem follows.

References

[Fa] G. Faltings: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Inv. Math.* 73 (1983).

[Ma] B. Mazur: Modular curves and the Eisenstein Ideal. *Publ. Math. IHES* 47 (1977).

[Ogg] A. Ogg: Diophantine equations and modular forms. *Bull AMS* 81 (1985).

(Oblatum 22-VIII-1985)

Fachbereich Mathematik
Fachbereich 9
Universität des Saarlandes
D-6600 Saarbrücken
BRD