CRITERIA FOR p-ORDINARITY OF FAMILIES OF ELLIPTIC CURVES OVER INFINITELY MANY NUMBER FIELDS

NUNO FREITAS AND PANAGIOTIS TSAKNIAS

ABSTRACT. Let K_i be a number field for all $i \in \mathbb{Z}_{>0}$ and let $\mathcal{E}$ be a family of elliptic curves containing infinitely many members defined over K_i for all i. Fix a rational prime p. We give sufficient conditions for the existence of an integer i_0 such that, for all $i > i_0$ and all elliptic curve $E \in \mathcal{E}$ having good reduction at all $\mathfrak{p} \mid p$ in K_i, we have that E has good ordinary reduction at all primes $\mathfrak{p} \mid p$.

We illustrate our criteria by applying it to certain Frey curves in [1] attached to Fermat-type equations of signature (r, r, p).

1. Introduction

Fix p a rational prime. Let K be a number field and for a prime $\mathfrak{p} \mid p$ write $f_\mathfrak{p}$ for its residual degree. Given an elliptic curve E/K with good reduction at $\mathfrak{p}$ we know that its trace of Frobenius at $\mathfrak{p}$ is given by the quatity

$$a_\mathfrak{p}(E) := (p^{f_\mathfrak{p}} + 1) - \#\tilde{E}(\mathbb{F}_{p^{f_\mathfrak{p}}}), \tag{1}$$

where $\tilde{E}$ is the reduction of E modulo $\mathfrak{p}$.

Let E/K be an elliptic curve given by a Weierstrass model with good reduction at all $\mathfrak{p} \mid p$ in K. It is simple to decide whether E is p-ordinary (i.e. has good ordinary reduction at all $\mathfrak{p} \mid p$). Indeed, for each $\mathfrak{p} \mid p$, compute $a_\mathfrak{p}(E)$ and check if $p \nmid a_\mathfrak{p}(E)$. If the previous holds for all $\mathfrak{p} \mid p$ then E is p-ordinary.

Now let $(E_\alpha/K)_{\alpha\in\mathbb{Z}^n}$ be a family of elliptic curves given by their Weierstrass models. Suppose that E_α has good reduction at all $\mathfrak{p} \mid p$ for all α. Write $\bar{\alpha} \in (\mathbb{Z}/p\mathbb{Z})^n$ for the reduction of α modulo p. We can naturally think of $\bar{\alpha} \in \mathbb{Z}^n$. Suppose further that $a_\mathfrak{p}(E_\alpha) = a_\mathfrak{p}(E_{\bar{\alpha}})$. We are interested in deciding whether E_α is p-ordinary for all α. This is also simple: using formula (1), we compute (the finitely many) $a_\mathfrak{p}(E_{\bar{\alpha}})$ for all $\bar{\alpha} \in (\mathbb{Z}/p\mathbb{Z})^n$ and all $\mathfrak{p} \mid p$ in K. Then, if p does not divide any of the previous values it follows that E_α is p-ordinary for all α.

A natural generalization is to consider the same question without the assumption that the E_α are all defined over the same field K. In this note we approach this question. Indeed, we will describe sufficient conditions (see Theorem 1) to establish p-ordinarity of a family of elliptic curves defined over varying fields.

A natural source of infinite families of elliptic curves is the application of the modular method to equations of Fermat-type $Ax^p + By^r = Cz^q$. Indeed, for certain particular cases of the previous equation, it is possible to attach to a solution $(a, b, c) \in \mathbb{Z}^3$ a Frey elliptic curve $E_{(a,b,c)}$ given by a Weierstrass model depending on a, b, c. This generates an infinite family of elliptic curves.

The first author was supported by a grant from Fundació Ferran Sunyer i Balaguer.
The second author was supported by the SPP 1489 priority program of the Deutsche Forschungsgemeinschaft.

Moreover, in [1] this method is applied to infinitely many equations generating a family of elliptic curves defined over varying fields. In section 3 below, we will use this family from [1] to illustrate our main result.

2. Main Theorem

For every $i \in \mathbb{Z}_{>0}$ let $K_i := \mathbb{Q}(z_i)$ be a number field. Let A be an indexing set. Consider a family of elliptic curves

$$\mathcal{E} := \{E_{\alpha,i} \,:\, \alpha \in A,\, i \in \mathbb{Z}_{>0}\}$$

where $E_{\alpha,i}$ is given by a Weierstrass model defined over K_i for all α. Write $c_4(E_{\alpha,i})$ and $\Delta(E_{\alpha,i})$ for the usual invariants attached to $E_{\alpha,i}$.

Fix a rational prime p. For every $i > 0$ let $A_i \subseteq A$ be the set of α for which $E_{\alpha,i}$ has good reduction at all $\mathfrak{p} \mid p$ in K_i. Suppose further that

(1) For all $i > 0$ and all $\alpha \in A_i$ there exist polynomials $C_\alpha, D_\alpha \in \mathbb{Z}_{(p)}[X]$ such that

$$C_\alpha(z_i) = c_4(E_{\alpha,i}) \quad \text{and} \quad D_\alpha(z_i) = \Delta(E_{\alpha,i}),$$

and

$$\max_\alpha\{\deg \overline{C}_\alpha\} < +\infty \quad \text{and} \quad \max_\alpha\{\deg \overline{D}_\alpha\} < +\infty$$

where $\overline{C}_\alpha$ and $\overline{D}_\alpha$ denote the corresponding mod p reductions.

(2) for $\alpha \in A_i$ the $\mathfrak{p}$-adic valuation of $\Delta(E_{\alpha,i})$ is 0 for all $\mathfrak{p} \mid p$ in K_i.

Our main theorem is then the following:

Theorem 1. *Let K_i and $E_{\alpha,i}$ be as above. Fix p to be a rational prime and for each $\mathfrak{p} \mid p$ in K_i let $f^i_{\mathfrak{p}}$ be the corresponding residual degree. Write f_i for the minimum of the $f^i_{\mathfrak{p}}$. Suppose that*

$$\lim_i f_i = +\infty.$$

Then, there exists a positive integer i_0 such that for all $i > i_0$ and all $\alpha \in A_i$ the elliptic curves $E_{\alpha,i}$ are ordinary at all primes $\mathfrak{p} \mid p$ in K_i.

Proof. Fix an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. For an element $\lambda \in \overline{\mathbb{F}}_p$ consider the elliptic curve E_λ : $y^2 = x(x-1)(x-\lambda)$. Write S_p for the set of roots of the Hasse polynomial $H_p(t)$. Write also

$$B_p := \{\, j(E_\lambda) \mid \lambda \in S_p \,\}.$$

From [3, Chapter V, Theorem 4.1] we know that B_p is the set of supersingular j-invariants modulo p. Moreover, from [3, Chapter V, Theorem 3.1] we have $B_p \subset \mathbb{F}_{p^2} \subseteq \overline{\mathbb{F}}_p$. Let E be an elliptic curve over a number field K, having good reduction at (all primes above) p. For a prime $\mathfrak{p} \mid p$ in K we write $\overline{j(E)}$ for $j(E) \pmod{\mathfrak{p}}$ seen as an element of $\overline{\mathbb{F}}_p$. Then, $\overline{j(E)} \neq b$ for all $b \in B_p$ implies that E is ordinary at $\mathfrak{p}$.

For the rest of the proof we fix a prime $\mathfrak{p}$ over p for each K_i. Thus, we have that for $\alpha \in A_i$ the curve $E_{(\alpha,i)}$ is ordinary at $\mathfrak{p}$ if

$$j(E_{\alpha,i}) = \frac{c_4(E_{\alpha,i})^3}{\Delta(E_{\alpha,i})} = \frac{\overline{C}_\alpha(\overline{z_i})^3}{\overline{D}_\alpha(\overline{z_i})} \neq b$$

for all $b \in B_p$, where $\overline{z}_i := z_i \pmod{\mathfrak{p}}$ seen as an element of $\overline{\mathbb{F}}_p$.

Set

$$d := \max_{\substack{b\in B_p\\ \alpha\in\cup_{i>0}A_i}} \{\deg(\overline{C}_\alpha(X)^3 - b\overline{D}_\alpha(X))\}, \tag{2}$$

By assumption d is finite, so there is a constant i_0 such that $f_i > d$ ($2d$ if B_p actually contains elements of $\mathbb{F}_p^2$ that are not in $\mathbb{F}_p$; the $f_\mathfrak{p}^i$'s are residual degrees over $\mathbb{F}_p$) for all $i > i_0$. Suppose now that $E_{\alpha,j}$ over K_j satisfies

$$\overline{C}_\alpha(\overline{z}_j)^3 - b\overline{D}_\alpha(\overline{z}_j) = 0$$

Then, the residual degree $f_\mathfrak{p}^j$ of K_j at $\mathfrak{p}$ is at most d (resp. $2d$), hence $j \leq i_0$. Thus, for all $i > i_0$, all $b \in B_p$ we have that

$$\overline{C}_\alpha(\overline{z}_i)^3 - b\overline{D}_\alpha(\overline{z}_i) \neq 0 \quad \Leftrightarrow \quad \frac{\overline{C}_\alpha(\overline{z}_i)^3}{\overline{D}_\alpha(\overline{z}_i)} \neq b.$$

for any choice of $\mathfrak{p}$ in K_i above p and therefore we conclude that for all $i > i_0$, the curve $E_{(\alpha,i)}$ is ordinary at p for all $\alpha \in A_i$.

□

Remark 2. We can obtain an even smaller d and therefore i_0 if we let d me the maximum among the degrees of the irreducible factors of the polynomials $\overline{C}_\alpha(X)^3 - b\overline{D}_\alpha(X)$ over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$ depending on where b lies. If one has an explicit enough description of the residual degrees for the fields K_i one can turn this in to an algorithm for explicitly computing i_0. This will be illustrated in the example below (see Theorem 3).

3. Application

First let us remark that the sequence of fields $\mathbb{Q}(\zeta_r)$, indexed by rational primes r, with ζ_r an r-th primitive root of unity, satisfy the conditions of the Main Theorem. With this in mind we have the following application of our Main Theorem:

Theorem 3. *Let $K_r = \mathbb{Q}(\zeta_r)^+$ be the maximal totally real subfield of $\mathbb{Q}(\zeta_r)$. Define*

$$E_{(a,b),r} := E^k_{(a,b)}/K_r,$$

where $k = (1,2,3)$ or $k = (1,2,4)$ and the definition of $E^k_{(a,b)}$ is as in [1]. Then, $E_{(a,b),r}$ is 3-ordinary for all primes $r > 7$ and all non-zero pairs $(a,b) \in \mathbb{Z}^2$.

Proof of Theorem 3: One needs to check that the fields K_r and the families of elliptic curves $E_{(a,b),r}$ satisfy indeed the hypotheses of Theorem 1:

- The fields K_r and $\mathbb{Q}(\zeta_r)$ are Galois and therefore the residue class degrees at 3 are all equal to the minimum. Write f_r and g_r for the residue class degree at 3 of K_r and $\mathbb{Q}(\zeta_r)$, respectively. One has (see for example [2, p. 35]) that g_r is the smallest positive integer g such that $r | 3^g - 1$. This clearly implies that $\lim_r g_r = +\infty$. Since g_r is equal to f_r or $2f_r$ one has the corresponding property for the fields K_r as well.
- $K_r = \mathbb{Q}(\xi_r)$ where $\xi_r = \zeta_r + \zeta_r^{-1}$. The model (described in [1, Section 2.3]) for each curve $E_{(a,b),r}$ is given by an equation for which $c_4(E_{(a,b),r}) = 2^4(AB+BC+AC)$ and $\Delta(E_{(a,b),r}) = 2^4(ABC)^2$ where A, B and C are given by polynomials in $\mathbb{Q}[X, Y_1, Y_2]$ evaluated at ξ_r, a, b and therefore the same holds for c_4 and Δ. It is also clear from the expressions that they actually lie in $\mathbb{Z}_{(3)}[a, b, \xi_r]$. We therefore have that for fixed (integer) parameters a, b the

parameters c_4 and Δ are in indeed given by polynomials in $C_{(a,b)}, D_{(a,b)} \in \mathbb{Z}_{(3)}[X]$ evaluated at ξ_r.

- The boundedness condition on the degrees of $\overline{C}_{(a,b)}$ and $\overline{D}_{(a,b)}$ as we let a and b vary is also evident from the fact that $C_{(a,b)}(X), D_{(a,b)}(X) \in \mathbb{Z}_{(3)}[a,b][X]$; varying a and b matters only up to reduction mod 3.
- Good reduction for the curves with a or $b \not\equiv 0 \pmod 3$ at primes above 3 is proven in [1, Proposition 3.2]. In other words, $A_i = \mathbb{Z}^2 \backslash (3\mathbb{Z})^2$ for all i.

Theorem 1 thus implies that there is a constant r_0 such that for all $r > r_0$ all the curves are ordinary at all primes above 3. Our goal now is to make this constant explicit, i.e. show that $r_0 = 7$. We proceed as outlined in Remark 2. From here onwards $\mathfrak{p}$ will denote a prime above 3.

For $p = 3$ we have that $B_3 = \{0\} \subseteq \mathbb{F}_3$. Thus one needs to check that $c_4^3 \not\equiv 0 \mod \mathfrak{p}$ or equivalently that $c_4 \not\equiv 0 \mod \mathfrak{p}$. The last one is true if and only if

$$AB + BC + AC \not\equiv 0 \pmod{\mathfrak{p}}. \tag{3}$$

Since $A + B + C = 0$, using the identity

$$(A + B + C)^2 = A^2 + B^2 + C^2 + 2(AB + AC + BC)$$

we get that conguence (3) is equivalent to

$$A^2 + B^2 + C^2 \not\equiv 0 \pmod{\mathfrak{p}}. \tag{4}$$

Notice that $AB + BC + AC \pmod{\mathfrak{p}}$ depends only on $(a, b) \pmod 3$ so we will assume from now on that $(a, b) \in \mathbb{F}_3^2 \backslash \{(0, 0)\}$. Furthermore, by the symmetry of A, B, C, it is enough to consider only the cases where $(a, b) \in \{(1, 0), (1, 1), (1, 2)\}$. Assume for now (which is going to be true for the cases we will consider) that we can find u, v, w such that

$$A = v - w, \quad B = w - u, \quad C = u - v. \tag{5}$$

Then congruence (4) is equivalent to

$$(v - w)^2 + (w - u)^2 + (u - v)^2 \not\equiv 0 \pmod{\mathfrak{p}}. \tag{6}$$

Since $\mathfrak{p} \mid 3$ we have that $u^3 + v^3 + w^3 \equiv (u + v + w)^3 \pmod{\mathfrak{p}}$ and therefore

$$u + v + w \not\equiv 0 \pmod{\mathfrak{p}}, \tag{7}$$

is equivalent to $u^3 + v^3 + w^3 \not\equiv 0 \pmod{\mathfrak{p}}$. Furthermore, using the identity

$$u^3 + v^3 + w^3 = \frac{1}{2}(u + v + w)\left[(w - v)^2 + (u - w)^2 + (v - u)^2\right] + 3uvw,$$

we see that congruence (7) implies congruence (6). The values of u, v and w in each of the three cases for (a, b) are:

- **The case** $(a, b) = (1, 0)$**.** In this case we have

$$A = \xi_{k_3} - \xi_{k_2}, \quad B = \xi_{k_1} - \xi_{k_3}, \quad C = \xi_{k_2} - \xi_{k_1}$$

  and it is trivial to see that

$$u = \xi_{k_1}, \quad v = \xi_{k_2}, \quad w = \xi_{k_3}.$$

- **The case** $(a, b) = (1, 1)$**.** In this case we have

$$A = (\xi_{k_3} - \xi_{k_2})(2 + \xi_{k_1}), \quad B = (\xi_{k_1} - \xi_{k_3})(2 + \xi_{k_2}), \quad C = (\xi_{k_2} - \xi_{k_1})(2 + \xi_{k_3})$$

  and it is easy to see that

$$u = \xi_{k_2}\xi_{k_3} - 2\xi_{k_1}, \quad \xi_{k_1}\xi_{k_3} - 2\xi_{k_2}, \quad w = \xi_{k_1}\xi_{k_2} - 2\xi_{k_3}.$$

- **The case** $(a, b) = (1, 2)$**.** In this case we have
  $A = (\xi_{k_3} - \xi_{k_2})(5 + 2\xi_{k_1}), \quad B = (\xi_{k_1} - \xi_{k_3})(5 + 2\xi_{k_2}), \quad C = (\xi_{k_2} - \xi_{k_1})(5 + 2\xi_{k_3})$
  and it is easy to see that
  $$u = 2\xi_{k_2}\xi_{k_3} - 5\xi_{k_1}, \quad v = 2\xi_{k_1}\xi_{k_3} - 5\xi_{k_2}, \quad w = 2\xi_{k_1}\xi_{k_2} - 5\xi_{k_3}.$$

It is easy to see that one can write $u + v + w$ as $h(\xi_1)$ with $h(X) \in \mathbb{Z}[X]$ using the identities:

$$\xi_k = \xi_1^k - \sum_{j=1}^{\lfloor k/2 \rfloor} \binom{k}{j} \xi_{k-2j} \quad \text{for } k \text{ odd and}$$

$$\xi_k = \xi_1^k - \sum_{j=1}^{k/2-1} \binom{k}{j} \xi_{k-2j} - \binom{k}{k/2} \quad \text{for } k \text{ even.}$$

Notice that the degree of h depends on the triple (k_1, k_2, k_3) and (a, b) but not on r.

Assume now that congruence (7) is not true, i.e. that $h(\xi_i) \equiv 0 \pmod{\mathfrak{p}}$. Then $g(\zeta_r) \equiv 0 \pmod{\mathfrak{p}}$ where $g(X) \in \mathbb{Z}[X]$ is the polynomial $X^{\deg(h)} h(X + 1/X)$, of degree $d = 2\deg(h)$, still independent of r. This implies that the extension $\mathbb{F}_3[\overline{\zeta_r}]/\mathbb{F}_3$ is of degree at most d.

The relation $r | 3^f - 1$ implies that, for a fixed f, there are only finitely many r, easily explicitly determined, such that the residue class degree is (at most) f. To finish things, we just have to examine what happens at these exceptional r. We will do this for $(a, b) = (1, 1)$ and $(k_1, k_2, k_3) = (1, 2, 3)$: In this case h is of degree 5 and it factors in $\mathbb{F}_3[X]$ as

$$(1 + X)(2 + X)(2 + X + X^2 + X^3).$$

The only primes $r \geq 7$ for which the extension $\mathbb{F}_3[\zeta_r]/\mathbb{F}_3$ is of degree at most 6 are 7, 11 and 13. One then verifies computationally for these primes that the Frey curve is indeed 3-ordinary, except for 7. We again look at (the prime divisors of) the norm of $u + v + w$:

- $r = 7$: The norm is 0.
- $r = 11$: The norm is 11^2.
- $r = 13$: The norm is 13^2.

The other cases are treated the same way and it turns out that $r > 7$ is the sufficient condition for both triples. □

References

[1] Nuno Freitas. Recipes for Fermat-type equations of signature (r, r, p) (preprint). http://arxiv.org/abs/1203.3371.

[2] J. S. Milne. Class field theory (v4.01), 2011. Available at www.jmilne.org/math/.

[3] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

E-mail address: Nuno.Freitas@uni-bayreuth.de

Department of Mathematics, University of Luxembourg, Campus Kirchberg, 6 rue Richard Coudenhove-Kalergi, L-1359 Luxembourg

E-mail address: panagiotis.tsaknias@uni.lu

E-mail address: p.tsaknias@gmail.com