PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 144, Number 1, January 2016, Pages 55–63
http://dx.doi.org/10.1090/proc12717
Article electronically published on July 1, 2015

# ON THE SINGULARITY OF THE DEMJANENKO MATRIX OF QUOTIENTS OF FERMAT CURVES

FRANCESC FITÉ AND IGOR E. SHPARLINSKI

(Communicated by Matthew A. Papanikolas)

Abstract. Given a prime $\ell \geq 3$ and a positive integer $k \leq \ell - 2$, one can define a matrix $D_{k,\ell}$, the so-called Demjanenko matrix, whose rank is equal to the dimension of the Hodge group of the Jacobian $\mathrm{Jac}(\mathcal{C}_{k,\ell})$ of a certain quotient of the Fermat curve of exponent $\ell$. For a fixed $\ell$, the existence of $k$ for which $D_{k,\ell}$ is singular (equivalently, for which the rank of the Hodge group of $\mathrm{Jac}(\mathcal{C}_{k,\ell})$ is not maximal) has been extensively studied in the literature. We provide an asymptotic formula for the number of such $k$ when $\ell$ tends to infinity.

## 1. Introduction

For a prime $\ell \geq 3$ and a positive integer $k \leq \ell - 2$, define the set

$$M_{k,\ell} := \{j \in (\mathbb{Z}/\ell\mathbb{Z})^* \mid \langle kj \rangle_\ell + \langle j \rangle_\ell < \ell\},$$

where, for $j \in (\mathbb{Z}/\ell\mathbb{Z})^*$, we denote by $\langle j \rangle_\ell$ the unique integer representative of $j$ modulo $\ell$ in the range $1, \ldots, \ell - 1$. This is a set of cardinality $(\ell-1)/2$. Using some results of Koblitz and Rohrlich [KR78, Theorem 2] one can show that the subgroup

$$W_{k,\ell} := \{w \in (\mathbb{Z}/\ell\mathbb{Z})^* \mid wM_{k,\ell} = M_{k,\ell}\}$$

of elements stabilizing $M_{k,\ell}$ has cardinality 3 or 1 depending on whether the parameter $k$ is a primitive cubic root of unity modulo $\ell$ or not; see [FGL14, Lemma 2.7]. The *Demjanenko matrix* is then defined as

$$D_{k,\ell} := \left(E_{k,\ell}(-c^{-1}a) - \frac{1}{2}\right)_{c,a \in M_{k,\ell}/W_{k,\ell}},$$

where

$$E_{k,\ell}(a) := \begin{cases} 0 & \text{if } a \in M_{k,\ell}, \\ 1 & \text{if } a \notin M_{k,\ell}. \end{cases}$$

Consider now the curve

$$\mathcal{C}_{k,\ell}: \quad V^\ell = U(U+1)^{\ell-k-1}.$$

This is a curve of genus $(\ell-1)/2$ that may be obtained as a quotient of the *Fermat curve* $\mathcal{F}_\ell : Y^\ell = X^\ell + 1$ by a certain subgroup of automorphisms of $\mathcal{F}_\ell$; we refer to [FGL14] for details. The fact that the rank of $D_{k,\ell}$ coincides with the dimension of the Hodge group of the Jacobian of $\mathcal{C}_{k,\ell}$ has been exploited in [FGL14] to determine the distribution of Frobenius traces attached to $\mathcal{C}_{k,\ell}$ when $D_{k,\ell}$ is non-singular.

Received by the editors June 14, 2014 and, in revised form, December 10, 2014.
2010 *Mathematics Subject Classification.* Primary 11G20, 11T24.
*Key words and phrases.* Fermat curve, Demjanenko matrix, Sato-Tate conjecture.

Let $\mathcal{K}_\ell$ denote the set of positive integers $k \le \ell-2$ for which $D_{k,\ell}$ is singular. It is easy to see that for every $\ell \equiv 2 \pmod 3$, the set $\mathcal{K}_\ell$ is empty (see Lemma 6). Lenstra has shown (see [Gre80, p. 354]) that $\mathcal{K}_\ell$ is non-empty for every sufficiently large $\ell \equiv 7 \pmod{12}$. In this note, we give an asymptotic formula for the cardinality of $\mathcal{K}_\ell$, which, in particular, shows that $\mathcal{K}_\ell$ is non-empty for an overwhelming majority of primes $\ell \equiv 1 \pmod 3$.

**Theorem 1.** *Let $\ell - 1 = 2^\alpha 3^\beta m$ for some integers $\alpha > 0$, $\beta \ge 0$ and $m$ with $\gcd(m,6) = 1$. Then*

$$\left| \#\mathcal{K}_\ell - \frac{1}{2^{2\alpha+2}} \left(1 - \frac{1}{3^{2\beta}}\right) \ell \right| \le 4\beta^2 \sqrt{\ell} + \frac{33}{16}\,.$$

The key result to prove Theorem 1 is the characterisation of the non-singularity of $D_{k,\ell}$ in terms of certain conditions on the multiplicative orders of $k$ and $k^2+k$ modulo $\ell$ obtained in [FGL14] (see Lemma 6 below).

**Corollary 2.** *Let $\ell-1 = 2^\alpha 3^\beta m$ for some integers $\alpha, \beta > 0$ and $m$ with $\gcd(m,6) = 1$. If $\ell > 441 \cdot 2^{4\alpha}\beta^4$, then $\#\mathcal{K}_\ell > 0$.*

The previous result can be verified by direct calculations for $\ell \le 7$, and for $\ell > 11$ it follows from the inequalities

$$\frac{1}{2^{2\alpha+2}} \left(1 - \frac{1}{3^{2\beta}}\right) \ell \ge \frac{1}{2^{2\alpha-1}9} \ell$$

and

$$4\beta^2\sqrt{\ell} + \frac{33}{16} < \left(4 + \frac{33}{16\sqrt{11}}\right) \beta^2 \sqrt{\ell} \le \left(4 + \frac{2}{3}\right) \beta^2 \sqrt{\ell}.$$

We can now obtain an explicit form of the observation of Lenstra.

**Corollary 3.** *For every prime $\ell \equiv 7 \pmod{12}$ distinct from 7 and 19 we have $\#\mathcal{K}_\ell > 0$.*

This can be deduced from Corollary 2 in the following way. First note that $\alpha = 1$. Observe that for

$$m \ge m_\beta := \lceil 441 \cdot 2^3 \cdot 3^{-\beta} \beta^4 \rceil\,,$$

we have that

$$\ell = 2 \cdot 3^\beta m \tag{1}$$

satisfies the hypothesis of Corollary 2 and thus $\#K_\ell > 0$. Since for $\beta \ge 18$, one has $m_\beta = 1$, we can limit our search for primes $\ell \equiv 7 \pmod{12}$ with $\#\mathcal{K}_\ell = 0$ among the finite set of primes $\ell$ of the form (1) with

$$\beta \in \{1, \dots, 17\} \qquad \text{and} \qquad m \le m_\beta - 1 \text{ with } \gcd(m,6) = 1.$$

A computer search establishes that the only primes of this form are

$$7, 19, 163, 487, 1459, 39367, 86093443, 258280327\,.$$

Among the above primes, we have $\#\mathcal{K}_\ell = 0$ only for $\ell = 7, 19$.

As we have mentioned, Lemma 6 below immediately implies that if $\ell \not\equiv 1 \pmod 3$, then $\mathcal{K}_\ell = \emptyset$. This is consistent with the vanishing of the main term of Theorem 1 for $\beta = 0$. We also use Corollary 2 to derive a bound on the density of primes $\ell \equiv 1 \pmod 3$ with $\mathcal{K}_\ell = \emptyset$.

**Theorem 4.** *For $x \geq 2$ there are at most $O(x^{3/4} \log x)$ primes $\ell \equiv 1 \pmod 3$ with $\ell \leq x$ and $\#\mathcal{K}_\ell = 0$.*

We cannot answer the question of whether there exist infinitely many primes $\ell \equiv 1 \pmod 3$ with $\#\mathcal{K}_\ell = 0$. However, we provide a reason to believe so. Indeed, standard heuristic arguments suggest that for any $\beta \geq 1$ and $m \geq 1$ with $\gcd(m, 6) = 1$ there are infinitely many primes of the form $\ell = 2^\alpha 3^\beta m + 1$, with $\alpha > 0$, and we now show that $\#\mathcal{K}_\ell = 0$ for most such primes. To this aim, for fixed integers $\beta \geq 0$ and $m \geq 1$ with $\gcd(m, 6) = 1$, we define $\mathcal{L}_{\beta,m}$ to be the set of primes of the form $\ell = 2^\alpha 3^\beta m + 1$, for some $\alpha > 0$, such that $\#\mathcal{K}_\ell > 0$. Then we have the following finiteness result.

**Theorem 5.** *For any fixed $\beta \geq 0$ and $m \geq 1$ such that $(m, 6) = 1$, the set $\mathcal{L}_{\beta,m}$ is finite. More precisely, if $\beta = 0$, then $\#\mathcal{L}_{\beta,m} = 0$, and we have*

$$\#\mathcal{L}_{\beta,m} = O\left(3^{2\beta} m^2/\beta\right)$$

*for $\beta \geq 1$.*

## 2. Preparations

Let $\operatorname{ord}_\ell k$ denote the multiplicative order of $k$ modulo $\ell$. Also for a prime $p$ and an integer $m$ we denote by $\nu_p(m)$ the $p$-adic order of $m$, that is, the largest integer $\nu$ with $p^\nu \mid m$. Our main tool is the following characterisation of the elements of $\mathcal{K}_\ell$ given in [FGL14].

**Lemma 6.** *For a prime $\ell \geq 3$ and a positive integer $k \leq \ell - 2$, we have $k \in \mathcal{K}_\ell$ if and only if the three following conditions hold:*

(i) $\operatorname{ord}_\ell k \neq 3$;
(ii) $\nu_2(\operatorname{ord}_\ell k) = \nu_2(\operatorname{ord}_\ell(-k^2 - k)) = 0$;
(iii) $\nu_3(\operatorname{ord}_\ell k) > \nu_3(\operatorname{ord}_\ell(k^2 + k))$.

Now, let $\mathcal{X}_\ell$ denote the group of multiplicative characters modulo $\ell$. Furthermore, let $\mathcal{X}_{\ell,d}$ denote the set of characters of order dividing $d$, that is, the set of characters $\chi \in \mathcal{X}_\ell$ such that $\chi^d = \chi_0$, where $\chi_0$ is the principal character; see [IK04, Chapter 3] for a background on characters. We also use $\mathcal{X}^*_{\ell,d}$ to denote the set of non-principal characters of $\mathcal{X}_{\ell,d}$. Given $\chi \in \chi_\ell$, we extend it to $\mathbb{F}_\ell$ in the following way: if $\chi = \chi_0$ is principal, then set $\chi_0(0) := 1$. Otherwise, set $\chi(0) := 0$.

Since $\mathcal{X}_\ell$ is dual to the multiplicative group $\mathbb{F}^*_\ell$ of the finite field of $\ell$ elements, for any divisor $t \mid \ell - 1$ and $u \in \mathbb{F}^*_\ell$, for $d = (\ell - 1)/t$ we have

$$\frac{1}{d} \sum_{\chi \in \mathcal{X}_{\ell,d}} \chi(u) = \begin{cases} 1, & \text{if } u^t = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

Finally, we recall the following special case of the Weil bound of character sums (see [IK04, Theorem 11.23]).

**Lemma 7.** *For any polynomial $Q(X) \in \mathbb{F}_\ell[X]$ with $N$ distinct zeros in the algebraic closure $\overline{\mathbb{F}}_\ell$ of $\mathbb{F}_\ell$ and which is not a perfect $s$th power in $\overline{\mathbb{F}}_\ell[X]$ for an integer $s \geq 2$, and a non-principal character $\chi \in \mathcal{X}^*_\ell$ of order $s$, we have*

$$\left| \sum_{k \in \mathbb{F}_\ell} \chi\left(Q(k)\right) \right| \leq (N - 1)\ell^{1/2}.$$

## 3. Proof of Theorem 1

Since condition (i) of Lemma 6 fails to hold for at most two integers $k \in [1, \ell-2]$ we have

$$|\#\mathcal{K}_\ell - \#\mathcal{K}_\ell^*| \le 2, \tag{3}$$

where $\mathcal{K}_\ell^*$ is the set of integers $k \in [1, \ell-2]$ satisfying conditions (ii) and (iii) of Lemma 6.

Let $\zeta(u)$ be the characteristic function of the condition $\nu_2(\operatorname{ord}_\ell u) = 0$. This is equivalent to

$$\operatorname{ord}_\ell u \mid 3^\beta m = (\ell-1)/2^\alpha.$$

So, we see from (2) that

$$\zeta(u) = \frac{1}{2^\alpha} \sum_{\chi \in \mathcal{X}_{\ell,2^\alpha}} \chi(u) = \frac{1}{2^\alpha} + \frac{1}{2^\alpha} \sum_{\chi \in \mathcal{X}^*_{\ell,2^\alpha}} \chi(u). \tag{4}$$

Furthermore, for a non-negative integer $h$, let $\eta_h(u)$ be the characteristic function of the condition $\nu_3(\operatorname{ord}_\ell u) = h$. This is equivalent to

$$\operatorname{ord}_\ell u \mid 2^\alpha 3^h m = \frac{\ell-1}{3^{\beta-h}} \qquad \text{and} \qquad \operatorname{ord}_\ell u \nmid 2^\alpha 3^{h-1} m = \frac{\ell-1}{3^{\beta-h+1}}.$$

So, we see from (2) that

$$\begin{aligned} \eta_h(u) &= \frac{1}{3^{\beta-h}} \sum_{\chi \in \mathcal{X}_{\ell,3^{\beta-h}}} \chi(u) - \frac{1}{3^{\beta-h+1}} \sum_{\chi \in \mathcal{X}_{\ell,3^{\beta-h+1}}} \chi(u) \\ &= \frac{2+\vartheta_h}{3^{\beta-h+1}} + \frac{1}{3^{\beta-h}} \sum_{\chi \in \mathcal{X}^*_{\ell,3^{\beta-h}}} \chi(u) - \frac{1}{3^{\beta-h+1}} \sum_{\chi \in \mathcal{X}^*_{\ell,3^{\beta-h+1}}} \chi(u), \end{aligned} \tag{5}$$

where in the case $h = 0$ we define $\mathcal{X}^*_{\ell,3^{\beta+1}} = \emptyset$ and we also set $\vartheta_0 = 1$ and $\vartheta_h = 0$ for $h \ge 1$.

Then we have

$$\#\mathcal{K}_\ell^* = \sum_{k=1}^{\ell-2} \mathcal{B}_{k,\ell} = \sum_{k \in \mathbb{F}_\ell} \mathcal{B}_{k,\ell} - \mathcal{B}_{0,\ell} - \mathcal{B}_{-1,\ell}\,, \tag{6}$$

where

$$\mathcal{B}_{k,\ell} := \zeta(k)\zeta(-k^2-k) \sum_{r=1}^{\beta} \sum_{s=0}^{r-1} \eta_r(k)\eta_s(k^2+k).$$

Examining the expressions (4) and (5) we conclude that, after expanding, each product $\zeta(k)\zeta(-k^2-k)\eta_r(k)\eta_s(k^2+k)$ contains the constant term

$$\frac{1}{2^{2\alpha}} \cdot \frac{2+\vartheta_r}{3^{\beta-r-1}} \cdot \frac{2+\vartheta_s}{3^{\beta-s-1}} = \frac{1}{2^{2\alpha}} \cdot \frac{2}{3^{\beta-r-1}} \cdot \frac{2+\vartheta_s}{3^{\beta-s-1}}$$

(provided that $r \ge 1$ in our settings), which does not depend on $k$, and also several terms with products of the form

$$\chi_1(k)\chi_2(-k^2-k)\chi_3(k)\chi_4(k^2+k)$$

with some characters $\chi_1, \chi_2 \in \mathcal{X}_{\ell,2^\alpha}$, $\chi_3, \chi_4 \in \mathcal{X}_{\ell,3^{\beta-h}} \cup \mathcal{X}_{\ell,3^{\beta-h+1}}$ such that at least one of them is non-principal. Since multiplicative characters form a cyclic group

(see [IK04, Chapter 3]), we see that for some character $\chi$ of order $\ell-1$ and integers $f$, $g$, $h$ with $0 \le f, g < \ell-1$, $f+g>0$, $h=0,1$ we have

$$\chi_1(k)\chi_2(-k^2-k)\chi_3(k)\chi_4(k^2+k) = \chi\left(k^f(k^2+k)^g(-1)^h\right).$$

Consider the polynomial

$$P(\overline{X},\overline{Y},\overline{Z},\overline{T},\overline{U},\overline{V}) := P_1(\overline{X})P_2(\overline{Y})\sum_{r=1}^{\beta}\sum_{s=0}^{r-1} P_{3,r}(\overline{Z},\overline{T})P_{4,r,s}(\overline{U},\overline{V}),$$

where

$$P_1(\overline{X}) =: \frac{1}{2^\alpha} + \frac{1}{2^\alpha}\sum_{i=1}^{2^\alpha-1} X_i, \qquad P_2(\overline{Y}) := \frac{1}{2^\alpha} + \frac{1}{2^\alpha}\sum_{i=1}^{2^\alpha-1} Y_i,$$

$$P_{3,r}(\overline{Z},\overline{T}) := \frac{2}{3^{\beta-r+1}} + \frac{1}{3^{\beta-r}}\sum_{i=1}^{3^{\beta-r}-1} Z_{i,r} - \frac{1}{3^{\beta-r+1}}\sum_{i=1}^{3^{\beta-r+1}-1} T_{i,r},$$

$$P_{4,r,s}(\overline{U},\overline{V}) := \frac{2+\vartheta_s}{3^{\beta-s+1}} + \frac{1}{3^{\beta-s}}\sum_{i=1}^{3^{\beta-s}-1} U_{i,r,s} - \frac{1}{3^{\beta-s+1}}\sum_{i=1}^{3^{\beta-s+1}-1} V_{i,r,s},$$

and where $\overline{X},\overline{Y},\overline{Z},\overline{T},\overline{U},\overline{V}$ are vector indeterminates given by

- $\overline{X} := (X_i)$ and $\overline{Y} := (Y_i)$ for $1 \le i \le 2^\alpha - 1$;
- $\overline{Z} := (Z_{i,r})$ and $\overline{T} := (T_{i,r})$ for $1 \le i \le 3^{\beta-r}-1$ and $1 \le r \le \beta$;
- $\overline{U} := (U_{i,r,s})$ and $\overline{V} := (V_{i,r,s})$ for $1 \le i \le 3^{\beta-s}-1$, $0 \le s \le r-1$, and $1 \le r \le \beta$.

Let $a_0, a_1, \ldots, a_N$ be the set of coefficients of the polynomial $P$ with $a_0$ denoting the constant term. One observes that

$$\sum_{k\in\mathbb{F}_\ell} \mathcal{B}_{k,\ell} = \ell a_0 + \sum_{i=1}^{N} a_i \sum_{k\in\mathbb{F}_\ell} \chi_i\left(k^{f_i}(k^2+k)^{g_i}(-1)^{h_i}\right), \tag{7}$$

where for every $i = 1,\ldots,\ell-1$ we have that $0 \le f_i, g_i < \ell-1$, $f_i+g_i>0$ are integers, $h_i = 0,1$, and $\chi_i$ are characters of order $\ell-1$.

Note that, on the one hand, we have

$$\begin{aligned}
a_0 &= \frac{1}{2^{2\alpha}}\left(\sum_{r=1}^{\beta}\frac{2}{3^{2\beta-r+2}} + \sum_{r=1}^{\beta}\sum_{s=0}^{r-1}\frac{4}{3^{2\beta-r-s+2}}\right)\\
&= \frac{1}{2^{2\alpha}}\left(\sum_{r=1}^{\beta}\frac{2}{3^{2\beta-r+2}} + \sum_{r=1}^{\beta}\frac{4}{3^{2\beta-r+2}}\cdot\frac{3^r-1}{2}\right)\\
&= \frac{1}{2^{2\alpha}}\left(\sum_{r=1}^{\beta}\frac{2}{3^{2\beta-r+2}} + \sum_{r=1}^{\beta}\left(\frac{2}{3^{2\beta-2r+2}} - \frac{2}{3^{2\beta-r+2}}\right)\right)\\
&= \frac{1}{2^{2\alpha}}\cdot\frac{2}{3^{2\beta+2}}\cdot\sum_{r=1}^{\beta}9^r = \frac{1}{2^{2\alpha}}\cdot\frac{2}{3^{2\beta+2}}\cdot\frac{9^{\beta+1}-9}{8}.
\end{aligned}$$

Hence

$$a_0 = \frac{1}{2^{2\alpha+2}}\left(1-\frac{1}{3^{2\beta}}\right). \tag{8}$$

On the other hand, it is clear that the sum of the absolute values of the coefficients of $P$ is equal to the sum over $r$ and $s$ of the products of the sums of the absolute values of the coefficients of the polynomials $P_1$, $P_2$, $P_{3,r}$, and $P_{4,r,s}$. Note that the sum of the absolute values of the coefficients of $P_1$ or $P_2$ is 1, whereas the sum of the absolute values of the coefficients of $P_{3,r}$ or $P_{4,r,s}$ is bounded by 2. This yields the bound

$$\sum_{i=1}^{N} |a_i| \le \sum_{i=0}^{N} |a_i| \ \le 1 \cdot 1 \cdot \beta^2 \cdot 2 \cdot 2 = 4\beta^2 \,. \tag{9}$$

Putting (7), (8), and (9) toghether, it follows from Lemma 7 that

$$\left| \sum_{k \in \mathbb{F}_\ell} \mathcal{B}_{k,\ell} - \frac{\ell}{2^{2\alpha+2}} \left(1 - \frac{1}{3^{2\beta}}\right) \right| \le 4\beta^2 \sqrt{\ell} \,. \tag{10}$$

It is immediate that

$$\mathcal{B}_{0,\ell} = a_0 \,. \tag{11}$$

Furthermore, observe that

$$\begin{aligned} \mathcal{B}_{-1,\ell} = & \left( \frac{1}{2^\alpha} + \frac{1}{2^\alpha} \sum_{\chi \in \chi^*_{\ell,2^\alpha}} \chi(-1) \right) \frac{1}{2^\alpha} \sum_{r=1}^{\beta} \sum_{s=0}^{r-1} \frac{2+\vartheta_s}{3^{2\beta-s-r+2}} \\ & \cdot \left( 2 + \vartheta_r + 3 \sum_{\chi \in \chi^*_{\ell,3^{\beta-r}}} \chi(-1) - \sum_{\chi \in \chi^*_{\ell,3^{\beta-r+1}}} \chi(-1) \right) \\ = & \, (2^\alpha - 2) a_0 \,. \end{aligned} \tag{12}$$

For the last equality we have used that $\chi(-1) = 1$ if the order of $\chi$ is a power of 3, and the equality

$$\sum_{\chi \in \chi^*_{\ell,2^\alpha}} \chi(-1) = 2^\alpha - 3 \,.$$

Combining (6) and (10), (11) and (12), we obtain

$$\left| \#\mathcal{K}^*_\ell - \frac{\ell - 2^\alpha + 1}{2^{2\alpha+2}} \left(1 - \frac{1}{3^{2\beta}}\right) \right| \le 4\beta^2 \sqrt{\ell} \,.$$

Recalling (3) we obtain

$$\left| \#\mathcal{K}_\ell - \frac{\ell}{2^{2\alpha+2}} \left(1 - \frac{1}{3^{2\beta}}\right) \right| \le 4\beta^2 \sqrt{\ell} + 2 + \frac{2^\alpha - 1}{2^{2\alpha+2}} \left(1 - \frac{1}{3^{2\beta}}\right) \,.$$

Since

$$2 + \frac{2^\alpha - 1}{2^{2\alpha+2}} \left(1 - \frac{1}{3^{2\beta}}\right) \le \frac{33}{16}$$

for $\alpha = 1, 2, \ldots$, the result now follows.

## 4. Proof of Theorem 4

We see from Corollary 2 that if $\#\mathcal{K}_\ell = 0$, then $1/2^\alpha = O(\beta/\ell^{1/4})$. So for $m$ in the representation $\ell - 1 = 2^\alpha 3^\beta m$ we have

$$m = O\left(\frac{\ell}{2^\alpha 3^\beta}\right) = O\left(\frac{\ell^{3/4}\beta}{3^\beta}\right) = O(x^{3/4})\,. \tag{13}$$

The total number $L$ of such primes $\ell - 1 = 2^\alpha 3^\beta m$ can be estimated as

$$J \le \sum_{\substack{\alpha,\beta=1\\ 2^\alpha 3^\beta < x}}^{\infty} \pi(C2^\alpha 3^\beta x^{3/4}, 2^\alpha 3^\beta, 1)\,, \tag{14}$$

for some absolute constant $C > 0$ (that corresponds to the implied constant in (13)), where, as usual, for integers $a$ and $q \ge 1$, we use $\pi(z, q, a)$ to denote the number of primes $p \le z$ in the arithmetic progression $p \equiv a \pmod q$.

We now recall that by the *Brun-Titchmarsh* Theorem (see [IK04, Theorem 6.6]) we have

$$\pi(z, q, a) = O\left(\frac{z}{\varphi(q)\log(z/q)}\right)\,,$$

uniformly over integers $a$ and $q$ with $z > q \ge 1$, where, as usual, $\varphi(q)$ denotes the Euler function of $q$. Hence

$$\pi(C2^\alpha 3^\beta x^{3/4}, 2^\alpha 3^\beta, 1) = O\left(\frac{C2^\alpha 3^\beta x^{3/4}}{\varphi(2^\alpha 3^\beta)\log\left(x^{3/4}\right)}\right) = O\left(\frac{x^{3/4}}{\log x}\right)\,.$$

Substituting this bound in (14) and summing it over $O((\log x)^2)$ pairs of non-negative integers $(\alpha, \beta)$ with $2^\alpha 3^\beta \le x$, we obtain the result.

## 5. Proof of Theorem 5

Let us assume that $\beta \ge 1$ (otherwise the statement is immediate). Suppose that there exists $k \in \mathcal{K}_\ell$. Then Lemma 6 implies that

$$\operatorname{ord}_\ell k = 3^a d\,, \qquad \operatorname{ord}_\ell(-k^2 - k) = 3^b e\,,$$

where $1 \le a \le \beta$, $0 \le b \le a - 1$, and $d, e$ are divisors of $m$. Note that $d$ must be non-trivial if $a = 1$ and $e$ must be non-trivial if $b = 0$. Let $\Phi_m(X)$ denote the $m$th cyclotomic polynomial. Then $k$ is simultaneously a root of

$$p_{a,d}(X) := \Phi_{3^a d}(X) \qquad \text{and} \qquad q_{b,e}(X) := \Phi_{3^b d}(-X^2 - X)$$

modulo $\ell$. This means that $\ell$ divides the resultant

$$R_{a,b,d,e} := \operatorname{Res}(p_{a,d}, q_{b,e}).$$

Note that $p_{a,d}(X)$ and $q_{b,e}(X)$ have no roots in common. Indeed, let $\zeta$ be a root of $p_{a,d}(X)$ (and so a root of unity of order $3^a d$) that is also a root of $q_{b,e}(X)$. Then $\zeta$ must satisfy that $-\zeta^2 - \zeta = \eta$ or, equivalently,

$$\zeta + 1 = -\frac{\eta}{\zeta}\,,$$

where $\eta$ is root of unity of order $3^b e$. Note that if a root of unity plus 1 is again a root of unity, then this root of unity is a primitive cubic root of unity. This is a contradiction with the fact that we cannot have $a = 1$ and $d = 1$ simultaneously. Hence $R_{a,b,d,e} \ne 0$.

Furthermore, since all roots $\zeta$ of $p_{a,d}(X)$ have absolute value 1, we have

$$|R_{a,b,d,e}| = \prod_{\zeta:\ p_{a,d}(\zeta)=0} |q_{b,e}(\zeta)| = \exp\left(O(3^{a+b}\varphi(d)\varphi(e))\right),$$

where the product runs over the $\zeta \in \mathbb{C}$ such that $p_{a,d}(\zeta) = 0$ and, as before, $\varphi(q)$ denotes the Euler function of $q$. Note that if $\omega(t)$ is the number of distinct prime divisors of an integer $t \geq 2$, then one has the inequality $\omega(t)! \leq t$. Using Stirling's formula, we derive $\omega(t) = O(\log t/\log(1+\log t))$. Hence $R_{a,b,d,e}$ has at most

$$\omega(R_{a,b,d,e}) = O\left(\frac{3^{a+b}\varphi(d)\varphi(e)}{a+b}\right)$$

distinct prime divisors. Hence

$$\begin{aligned}\#\mathcal{L}_{\beta,m} &= O\left(\sum_{a=1}^{\beta}\sum_{b=0}^{a-1}\sum_{d|m}\sum_{e|m}\frac{3^{a+b}\varphi(d)\varphi(e)}{a+b}\right)\\ &= O\left(\sum_{a=1}^{\beta}\sum_{b=0}^{a-1}\frac{3^{a+b}}{a}m^2\right) = O\left(\sum_{a=2}^{\beta}\frac{3^{2a}}{a}m^2\right) = O\left(3^{2\beta}m^2/\beta\right).\end{aligned}$$

## 6. Comments

In addition to $\#\mathcal{L}_{0,m} = 0$ of Theorem 5 we also note that $\mathcal{L}_{1,1} = \mathcal{L}_{2,1} = \mathcal{L}_{3,1} = \emptyset$. Indeed, for $\mathcal{L}_{1,1}$ the statement is immediate. We now let $\mathcal{L}_{a,b,d,e}$ denote the set of primes dividing $R_{a,b,d,e}$. One computes

$$\mathcal{L}_{2,1,1,1} = \{3\}, \qquad \mathcal{L}_{3,2,1,1} = \{3, 271\}, \qquad \mathcal{L}_{3,1,1,1} = \{3, 271\}.$$

It remains to note that $\mathcal{K}_3 = 0$ and that 271 is not of the form $2^\alpha 3^3 + 1$ for any $\alpha$.

We now define $\ell_s$ as the smallest prime $\ell \equiv 1 \pmod 3$ with $\mathcal{K}_\ell = 0$ and $\omega(\ell-1) \geq s$ (if such prime exists), where, as before, $\omega(t)$ denotes the number of distinct prime divisors of an integer $t \geq 2$. From Theorem 5 we expect that in fact $\ell_s$ exists for any $s \geq 2$. In Table 1 we present some computational results which characterise the growth $\ell_s$.

Table 1. Values $\ell_s$ with $3 \leq s \leq 6$

| $s$ | $\ell_s$ | Factorization of $\ell_s - 1$ |
|---|---|---|
| 3 | 31 | $2 \cdot 3 \cdot 5$ |
| 4 | 3121 | $2^4 \cdot 3 \cdot 5 \cdot 13$ |
| 5 | 127681 | $2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 19$ |
| 6 | 25858561 | $2^9 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 37$ |

We have not found $\ell_7$, but our computation shows that if $\ell_7$ exists, then $\ell_7 > 31 \cdot 10^6$. On the other hand, combining the bound of Theorem 5 with the standard heuristic on the distribution on primes, one can derive a heuristic upper bound on $\ell_s$.

We remark that it is shown in [FGL14] that if $k$ satisfies the conditions of Lemma 6, that is, $k \in \mathcal{K}_\ell$, then the rank $\mathrm{rk}\,(D_{k,\ell})$ of the corresponding Demjanenko matrix satisfies

$$\mathrm{rk}\,(D_{k,\ell}) = \frac{\ell-1}{2}\left(1 - \frac{2}{M(k,\ell)}\right),$$

where

$$M(k,\ell) := \operatorname{lcm}\left[\operatorname{ord}_\ell\left(-k^2-k\right), \operatorname{ord}_\ell\left(k\right)\right].$$

The resultant argument of [FGL14] shows that

$$\min_{k\in\mathcal{K}_\ell} M(k,\ell) \to \infty$$

as $\ell \to \infty$. This can easily be sharpened as

$$\min_{k\in\mathcal{K}_\ell} M(k,\ell) \geq c\sqrt{\log \ell}$$

for an absolute constant $c > 0$. In fact the same argument shows that for any real function $\psi(z)$ with $\psi(z) \to 0$ as $z \to \infty$, all but $o(x/\log x)$ primes $\ell \leq x$, we have

$$\min_{k\in\mathcal{K}_\ell} M(k,\ell) \geq \psi(\ell)\ell^{1/3}.$$

Finally, we remark that our approach allows us to study the distribution of the values of $M(k,\ell)$ for every $\ell$.

## Acknowledgements

The interest for the proportion of $k \in [2, \ell-2]$ for which $D_{k,\ell}$ is singular arose after a question of Kiran Kedlaya during a talk by the first author at the Workshop "Frobenius distributions on curves" held at CIRM, Luminy, in February 2014. The authors are grateful to CIRM for its support and hospitality.

During the preparation the first author was funded by the German Research Council via CRC 701, and partially supported by MECD project MTM2012-34611; the second author was supported in part by ARC grant DP130100237.

## References

[FGL14] Francesc Fité, Josep González, Joan-Carles Lario, *Frobenius distribution for quotients of Fermat curves of prime exponent*, Canad. J. Math, to appear.

[Gre80] Ralph Greenberg, *On the Jacobian variety of some algebraic curves*, Compositio Math. **42** (1980/81), no. 3, 345–359. MR607375 (82j:14036)

[IK04] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004. MR2061214 (2005h:11005)

[KR78] Neal Koblitz and David Rohrlich, *Simple factors in the Jacobian of a Fermat curve*, Canad. J. Math. **30** (1978), no. 6, 1183–1205, DOI 10.4153/CJM-1978-099-6. MR511556 (80d:14022)

Institut für Experimentelle Mathematik/Fakultät für Mathematik, Universität Duisburg-Essen, D-45127 Essen, Germany

*E-mail address*: francesc.fite@gmail.com

Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia

*E-mail address*: igor.shparlinski@unsw.edu.au