BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 56, No. 3-4, 2008

NUMBER THEORY

The Analytic Rank of a Family of Jacobians of Fermat Curves

by

Tomasz JĘDRZEJAK

Presented by Andrzej BIAŁYNICKI-BIRULA

Summary. We study the family of curves $F_m(p) : x^p + y^p = m$, where p is an odd prime and m is a pth power free integer. We prove some results about the distribution of root numbers of the L-functions of the hyperelliptic curves associated to the curves $F_m(p)$. As a corollary we conclude that the jacobians of the curves $F_m(5)$ with even analytic rank and those with odd analytic rank are equally distributed.

1. Introduction. Let E be an elliptic curve over $\mathbb{Q}$ given by the equation $y^2 = x^3 + ax + b$ $(a, b \in \mathbb{Z})$. If d is a squarefree integer, then we define the dth quadratic twist E_d of E to be the elliptic curve defined by the equation $dy^2 = x^3+ax+b$. It is widely expected that for a given E the set of squarefree integers d such that $\operatorname{rank}(E_d(\mathbb{Q})) = 0$ has a positive density, but this is only known for special cases. Such an expectation follows, under the Riemann hypothesis, from the work of Iwaniec and Sarnak [5]. Conditional results in more general situations (including abelian varieties) are also proved in [2]. One can consider other families of elliptic curves (or abelian varieties) as well.

In general it is very difficult to calculate the rank of any specific elliptic curve (or abelian variety). It is much easier to treat the global root number $\varepsilon(A)$ of an abelian variety over $\mathbb{Q}$. Let us recall that the parity conjecture states that $\varepsilon(A) = (-1)^{r_A}$, where r_A denotes the rank of $\mathbb{Q}$-points of A.

Mai [6] showed that the set of cubefree natural numbers m for which the root number of $E^m : x^3 + y^3 = m$ is positive, has density $1/2$. The parity conjecture implies that in this family (of cubic twists of the Fermat curve

2000 *Mathematics Subject Classification*: 11G40, 11G10, 11G30, 11G35.
Key words and phrases: twisted Fermat curves, hyperelliptic curves, jacobian variety, L-function, root number, analytic rank.

DOI: 10.4064/bp56-3-2

$x^3 + y^3 = 1$) the rank of $\mathbb{Q}$-points of E^m is even for half of the cubefree natural numbers m.

In this article we will generalize the result of Mai to the family of curves $F_m(5) : x^5 + y^5 = m$ (Corollary 2).

According to the referee's suggestion, we will include the proof of a more general result (Theorem 1). The remaining part of the introduction contains definitions and constructions leading to the formulation of that result. We will consider the curve $F_m(p) : x^p + y^p = m$ (p is an odd prime) of genus $(p-1)(p-2)/2$. We also consider the curves of genus $(p-1)/2$

$$C_{m,s}(p) : y^p = x(m-x)^s \quad \text{for } s = 1, \dots, p-2.$$

The curves $C_{m,(p-1)/2}(p)$ and $C_{m,p-2}(p)$ are birationally equivalent; the corresponding map $C_{m,(p-1)/2}(p) \to C_{m,p-2}(p)$ is

$$(x,y) \mapsto \left(m - \frac{y^p}{(m-x)^{(p-1)/2}}, \frac{y^{p-2}}{(m-x)^{(p-3)/2}} \right).$$

For $s = 1, \dots, p-2$ we define the maps

$$\phi_{m,s} : F_m(p) \to C_{m,s}(p)$$

by the formula

$$\phi_{m,s}(x,y,1) = (x^p, xy^s, 1).$$

The map $\phi_{m,s}$ induces the well-defined map $J_m(p) \to J_{m,s}(p)$ between the corresponding jacobians. Similarly to [3], [4] we obtain the isogeny defined over $\mathbb{Q}$

$$\phi := \prod_{s=1}^{p-2} \phi_{m,s} : J_m(p) \to \prod_{s=1}^{p-2} J_{m,s}(p). \tag{1}$$

In particular, the problem of computing the rank of $J_m(5)(\mathbb{Q})$ reduces to calculating the ranks of $J_{m,s}(5)(\mathbb{Q})$ for $s = 1, 2$.

For $s = 1, (p-1)/2, p-2$ the curves $C_{m,s}(p)$ are hyperelliptic. By the substitution

$$(x,y) \mapsto \left(m - \left(\frac{4m}{x}\right)^p \left(\frac{y}{2^p m^{(p-1)/2}} - \frac{1}{2} \right), \left(\frac{4m}{x}\right)^{p-1} \left(\frac{y}{2^p m^{(p-1)/2}} - \frac{1}{2} \right) \right)$$

in the equation of $C_{m,p-2}(p)$ and $(x,y) \mapsto (y/2^p + m/2, -x/4)$ in the equation of $C_{m,1}(p)$ we obtain the hyperelliptic curves

$$A_{m,p} : y^2 = x^p + (4m)^{p-1}, \qquad B_{m,p} : y^2 = x^p + 4^{p-1}m^2.$$

We assume that m is a pth power free positive integer and $p \nmid m$.

2. Proof of the main result. Using the results of [8] we can calculate the sign of the functional equation of the L-functions of the hyperelliptic

curves $A_{m,p}$, $B_{m,p}$. Let

$$\mathbb{N}^{(p)} = \{m \in \mathbb{N} : p \nmid m,\ m \text{ is } p\text{th power free}\}.$$

For $m \in \mathbb{N}^{(p)}$ we put

$$\tau_p(m) = \#\left\{q \in \mathcal{P} : q > 2,\ q \mid m,\ \left(\frac{q}{p}\right) = -1\right\}.$$

Let $W_{m,p}$, $W^A_{m,p}$, $W^B_{m,p}$ denote the (global) root numbers of the curves $F_m(p)$, $A_{m,p}$, $B_{m,p}$ respectively. It turns out that $W^A_{m,p}$, $W^B_{m,p}$ (for fixed p and m) depend only on the parity of $\tau_p(m)$ and on the remainder of m modulo p^2. For example ($p = 5$, m odd)

$$W^A_{m,5} = (-1)^{\tau_5(m)+\varepsilon^A(m)}, \qquad W^B_{m,5} = (-1)^{\tau_5(m)+\varepsilon^B(m)},$$

where

$$\varepsilon^A(m) = \begin{cases} 0 & \text{for } m \equiv \pm1, \pm2, \pm7, \pm11 \pmod{25}, \\ 1 & \text{for } m \equiv \pm3, \pm4, \pm6, \pm8, \pm9, \pm12 \pmod{25}, \end{cases}$$

$$\varepsilon^B(m) = \begin{cases} 0 & \text{for } m \equiv \pm1, \pm3, \pm4, \pm7 \pmod{25}, \\ 1 & \text{for } m \equiv \pm2, \pm6, \pm8, \pm9, \pm11, \pm12 \pmod{25}. \end{cases}$$

THEOREM 1. *The sets* $\{m \in \mathbb{N}^{(p)} : W^A_{m,p} = 1\}$ *and* $\{m \in \mathbb{N}^{(p)} : W^B_{m,p} = 1\}$ *have density* $1/2$ *in the set* $\mathbb{N}^{(p)}$.

COROLLARY 2. *The set* $\{m \in \mathbb{N}^{(5)} : W_{m,5} = 1\}$ *has density* $1/2$ *in* $\mathbb{N}^{(5)}$.

Proof. From isogeny (1) we have $W_{m,5} = (W^A_{m,5})^2 W^B_{m,5} = W^B_{m,5}$. ∎

The proof of Theorem 1 splits into a few lemmas.

LEMMA 3. *For any Dirichlet character* χ *of conductor* k *we have*

$$\sum_{m \in \mathbb{N}^{(p)}_X} (-1)^{\tau_p(m)} \chi(m) = O(\sqrt{X} \log^{p-2} X \sqrt{k} \log k),$$

where $\mathbb{N}^{(p)}_X = \{m \in \mathbb{N}^{(p)} : m \le X\}$.

Proof. Each $m \in \mathbb{N}^{(p)}$ can be uniquely written in the form $n_1^{p-1} n_2^{p-2} \cdots n_{p-2}^2 n_{p-1}$, where the n_i are squarefree, pairwise coprime and not divisible by p. Then $\tau_p(m) = \tau_p(n_1) + \tau_p(n_2) + \cdots + \tau_p(n_{p-1})$, hence

$$\sum_{m \in \mathbb{N}^{(p)}_X} (-1)^{\tau_p(m)} \chi(m) = \sum_{\substack{n_1^{p-1} \cdots n_{p-1} \le X \\ n_i \text{ squarefree} \\ \text{and coprime} \\ p \nmid n_1 \cdots n_{p-1}}} \prod_{i=1}^{p-1} (-1)^{\tau_p(n_i)} \chi(n_i^{p-i}) = \sum_{\substack{n_1^{p-1} \cdots n_{p-1} \le X \\ n_i \text{ squarefree} \\ \text{and coprime}}} \prod_{i=1}^{p-1} \psi(n_i) \chi(n^{p-i}),$$

where $\psi(\cdot) = \left(\frac{\cdot}{p}\right)$ (therefore $\psi(x) = (-1)^{\tau_p(x)}$ for x squarefree not divisible by p). Let χ_a be the principal character modulo $2a$, i.e. $\chi_a(b) = 1$ if $(2a, b) = 1$, and 0 otherwise. Then

$$\begin{aligned}
&\sum_{m\in\mathbb{N}_X^{(p)}} (-1)^{\tau_p(m)}\chi(m)\\
&\quad= \sum_{\substack{n_1\le \sqrt[p-1]{X}\\ n_1 \text{ squarefree}}} \psi(n_1)\chi(n_1^{p-1})\chi_1(n_1) \sum_{\substack{n_2\le \sqrt[p-2]{X/n_1^{p-1}}\\ n_2 \text{ squarefree}}} \psi(n_2)\chi(n_2^{p-2})\chi_{n_1}(n_2)\\
&\qquad\times\cdots\times \sum_{\substack{n_{p-2}\le \sqrt{X}/\sqrt{n_1^{p-1}\cdots n_{p-3}^3}\\ n_{p-2} \text{ squarefree}}} \psi(n_2)\chi(n_2^2)\chi_{n_1\cdots n_{p-3}}(n_{p-2})\\
&\qquad\times \sum_{\substack{n_{p-1}\le X/n_1^{p-1}\cdots n_{p-2}^2\\ n_{p-1} \text{ squarefree}}} \psi(n_{p-1})\chi(n_{p-1})\chi_{n_1\cdots n_{p-2}}(n_{p-1}).
\end{aligned}$$

The last sum can be written in the form

$$\begin{aligned}
&\sum_{n_{p-1}\le X/n_1^{p-1}\cdots n_{p-2}^2} \psi(n_{p-1})\chi(n_{p-1})\chi_{n_1\cdots n_{p-2}}(n_{p-1}) \sum_{l^2|n_{p-1}} \mu(l)\\
&\qquad= \sum_{l\le \sqrt{X/n_1^{p-1}\cdots n_{p-2}^2}} \mu(l)\psi(l^2)\chi(l^2)\chi_{n_1\cdots n_{p-2}}(l^2)\\
&\qquad\quad\times \sum_{n'\le X/n_1^{p-1}\cdots n_{p-2}^2 l^2} \psi(n')\chi(n')\chi_{n_1\cdots n_{p-2}}(n').
\end{aligned}$$

Now we use the Pólya–Vinogradov inequality: If χ is the primitive character modulo $k > 2$, then $\sum_{n\le X}\chi(n) = O(\sqrt{k}\log k)$. It implies

$$\sum_{n'\le X/n_1^{p-1}\cdots n_{p-2}^2 l^2} \psi(n')\chi(n')\chi_{n_1\cdots n_{p-2}}(n') = O(\sqrt{k}\log k),$$

hence

$$\begin{aligned}
&\sum_{\substack{n_{p-1}\le X/n_1^{p-1}\cdots n_{p-2}^2\\ n_{p-1} \text{ squarefree}}} \psi(n_{p-1})\chi(n_{p-1})\chi_{n_1\cdots n_{p-2}}(n_{p-1})\\
&\qquad\qquad = O\left(\sqrt{\frac{X}{n_1^{p-1}\cdots n_{p-2}^2}}\sqrt{k}\log k\right).
\end{aligned}$$

Next by using the well-known estimate $\sum_{n\le X} 1/n = \log X + \gamma + O(1/X)$,

where $\gamma \approx 0.577$ is the Euler constant, we obtain successively

$$\begin{aligned}
&\sum_{m\in\mathbb{N}_X^{(p)}} (-1)^{\tau_p(m)}\chi(m)\\
&= \sum_{\substack{n_1\le \sqrt[p-1]{X}\\ n_1 \text{ squarefree}}} \psi(n_1)\chi(n_1^{p-1})\chi_1(n_1) \sum_{\substack{n_2\le \sqrt[p-2]{X/n_1^{p-1}}\\ n_2 \text{ squarefree}}} \psi(n_2)\chi(n_2^{p-2})\chi_{n_1}(n_2)\\
&\quad \times\cdots\times \sum_{\substack{n_{p-2}\le \sqrt{X}/\sqrt{n_1^{p-1}\cdots n_{p-3}^3}\\ n_{p-2} \text{ squarefree}}} O\biggl(\sqrt{\frac{X}{n_1^{p-1}\cdots n_{p-2}^2}}\sqrt{k}\log k\biggr)\\
&= \cdots = \sum_{\substack{n_1\le \sqrt[p-1]{X}\\ n_1 \text{ squarefree}}} \psi(n_1)\chi(n_1^{p-1})\chi_1(n_1)\\
&\quad \times \sum_{\substack{n_2\le \sqrt[p-2]{X/n_1^{p-1}}\\ n_2 \text{ squarefree}}} O\biggl(\sqrt{\frac{X}{n_1^{p-1}n_2^{p-2}}}\log\sqrt{X}\cdots\log\sqrt[p-3]{\frac{X}{n_1^{p-1}n_2^{p-2}}}\sqrt{k}\log k\biggr)\\
&= \sum_{\substack{n_1\le \sqrt[p-1]{X}\\ n_1 \text{ squarefree}}} O\biggl(\sqrt{\frac{X}{n_1^{p-1}}}\log\sqrt{X}\cdots\log\sqrt[p-2]{\frac{X}{n_1^{p-1}}}\sqrt{k}\log k\biggr)\\
&= O(\sqrt{X}\log\sqrt{X}\cdots\log\sqrt[p-2]{X}\log\sqrt[p-1]{X}\sqrt{k}\log k)\\
&= O(\sqrt{X}\log^{p-2}X\sqrt{k}\log k). \ \blacksquare
\end{aligned}$$

LEMMA 4. *The set $\mathbb{N}^{(p)}$ has a positive density in the set of natural numbers.*

Proof. Let p_n denote the nth prime. We define

$$a_n = \begin{cases} p_n & \text{if } p_n = p,\\ p_n^p & \text{if } p_n \ne p.\end{cases}$$

Then $(a_n, a_k) = 1$ for $n \ne k$, $\mathbb{N}^{(p)} = \{m \in \mathbb{N} : a_k \nmid m \text{ for every } k\}$, and the series $\sum_{n\in\mathbb{N}} 1/a_n$ converges. Recall that by Theorem 2.18 in [7] the density of $\mathbb{N}^{(p)}$ is

$$\prod_{n\in\mathbb{N}}\biggl(1-\frac{1}{a_n}\biggr) = \prod_{q\in\mathcal{P}}\biggl(1-\frac{1}{q^p}\biggr)\frac{1-1/p}{1-1/p^p} = \frac{1}{\zeta(p)}\,\frac{(p-1)p^{p-1}}{p^p-1}. \ \blacksquare$$

LEMMA 5. *The set $\{m \in \mathbb{N}^{(p)} : \tau_p(m)$ even$\}$ has density $1/2$ in $\mathbb{N}^{(p)}$.*

Proof. This follows from Lemma 3:

$$\sum_{\substack{m\in\mathbb{N}_X^{(p)}\\ \tau_p(m)\text{ even}}} 1 = \frac{1}{2}\sum_{m\in\mathbb{N}_X^{(p)}}(1+(-1)^{\tau_p(m)}) = \frac{1}{2}\sum_{m\in\mathbb{N}_X^{(p)}} 1 + O(\sqrt{X}\log^{p-2}X). \blacksquare$$

Proof of Theorem 1. Let C denote $A_{m,p}$ or $B_{m,p}$, and W_C be the sign of the functional equation of the L-function associated with C. Then

$$\sum_{\substack{m\in\mathbb{N}_X^{(p)}\\ W_C=1}} 1 = \sum_{\substack{m\in\mathbb{N}_X^{(p)}\\ \tau_p(m)\text{ even}\\ m\,(\mathrm{mod}\,p^2)\in U}} 1 + \sum_{\substack{m\in\mathbb{N}_X^{(p)}\\ \tau_p(m)\text{ odd}\\ m\,(\mathrm{mod}\,p^2)\in T}} 1,$$

where U and T are disjoint nonempty sets of integers modulo p^2 such that $U\cup T$ contains all numbers modulo p^2 nondivisible by p. Let $m\equiv k\,(\mathrm{mod}\,p^2)$, where $(k,p)=1$. Then by Lemma 3 we have

$$\begin{aligned}
\sum_{\substack{m\in\mathbb{N}_X^{(p)}\\ \tau_p(m)\text{ even}\\ m\equiv k\,(\mathrm{mod}\,p^2)}} 1 &= \sum_{\substack{m\in\mathbb{N}_X^{(p)}\\ \tau_p(m)\text{ even}}} \frac{1}{\phi(p^2)}\sum_{\chi\,(\mathrm{mod}\,p^2)}\chi(m)\overline{\chi}(k)\\
&= \frac{1}{p^2-p}\sum_{\chi\,(\mathrm{mod}\,p^2)}\overline{\chi}(k)\sum_{\substack{m\in\widetilde{\mathbb{N}}_X^{(p)}\\ \tau_p(m)\text{ even}}}\chi(m)\\
&= \frac{1}{2(p^2-p)}\sum_{\chi\,(\mathrm{mod}\,p^2)}\overline{\chi}(k)\sum_{m\in\mathbb{N}_X^{(p)}}\chi(m)(1+(-1)^{\tau_p(m)})\\
&= \frac{1}{2(p^2-p)}\sum_{\chi\,(\mathrm{mod}\,p^2)}\overline{\chi}(k)\sum_{m\in\mathbb{N}_X^{(p)}}\chi(m) + O(\sqrt{X}\log^{p-2}X)\\
&= \frac{1}{2(p^2-p)}\sum_{m\in\mathbb{N}_X^{(p)}}\sum_{\chi\,(\mathrm{mod}\,p^2)}\overline{\chi}(k)\chi(m) + O(\sqrt{X}\log^{p-2}X)\\
&= \frac{1}{2}\sum_{\substack{m\in\mathbb{N}_X^{(p)}\\ m\equiv k\,(\mathrm{mod}\,p^2)}} 1 + O(\sqrt{X}\log^{p-2}X).
\end{aligned}$$

In view of the above equalities (similar computations have to be done for

$\tau(m)$ odd with factor $1-(-1)^{\tau(m)}$) and Lemma 5 we obtain

$$\sum_{\substack{m\in\mathbb{N}_X^{(p)}\\ W_C=1}} 1 = \frac{1}{2}\sum_{\substack{m\in\mathbb{N}_X^{(p)}\\ m\,(\mathrm{mod}\,p^2)\in U}} 1 + \frac{1}{2}\sum_{\substack{m\in\mathbb{N}_X^{(p)}\\ m\,(\mathrm{mod}\,p^2)\in T}} 1 + O(\sqrt{X}\log^{p-2}X)$$
$$= \frac{1}{2}\sum_{m\in\mathbb{N}_X^{(p)}} 1 + O(\sqrt{X}\log^{p-2}X).$$

Now the assertion follows from Lemma 4. ∎

Remark. We note that if the curve $F_m(5)$ has an affine rational point (this occurs if m is a sum of two integer 5th powers), then the curves $A_{m,5}$, $B_{m,5}$ have nontrivial rational points. One can show that the rank of the groups $J_{A_{m,5}}(\mathbb{Q})$ and $J_{B_{m,5}}(\mathbb{Q})$ is at least 1. Taking into account the isogeny (1) we obtain $\mathrm{rank}(J_m(5)(\mathbb{Q})) \geq 3$. The set $\{a^5+b^5 : a\in\mathbb{N},\ a^5+b^5$ is 5th power free$\}$ ($b\in\mathbb{N}$ fixed) is infinite (even more: it can be proved by standard sieve methods to have a positive density), hence there are infinitely many nonisomorphic curves $x^5+y^5=m$ with $\mathrm{rank}(J_m(5)(\mathbb{Q}))\geq 3$. If additionally the sign of the functional equation of the L-functions of the curves $A_{m,5}$, $B_{m,5}$ is $+1$, then conjecturally $\mathrm{rank}(J_m(5)(\mathbb{Q}))\geq 6$. This happens e.g. for $m=33$. In [1] we prove that the unboundedness of ranks in the family $J_m(5)(\mathbb{Q})$ is equivalent to the divergence of certain infinite series.

Acknowledgements. I would like to thank Andrzej Dąbrowski for helpful conversations and suggestions. I am grateful to the referee for valuable comments.

References

[1] A. Dąbrowski and T. Jędrzejak, *Ranks in families of Jacobian varieties of twisted Fermat curves*, Canad. Math. Bull., to appear.

[2] A. Dąbrowski and J. Pomykała, *Nonvanishing of motivic L-functions*, Math. Proc. Cambridge Philos. Soc. 130 (2001), 221–235.

[3] D. K. Faddeev, *The group of divisor classes on some algebraic curves*, Soviet Math. Dokl. 2 (1961), 67–69.

[4] —, *Invariants of divisor classes for the curves $x^k(1-x)=y^l$ in the l-adic cyclotomic field*, Trudy Mat. Inst. Steklov. 64 (1961), 284–293 (in Russian).

[5] H. Iwaniec and P. Sarnak, *The non-vanishing of central values of automorphic L-functions and Landau–Siegel zeros*, Israel J. Math. 120 (2000), 155–177.

[6] L. Mai, *The analytic rank of a family of elliptic curves*, Canad. J. Math. 45 (1993), 847–862.

[7] W. Narkiewicz, *Number Theory*, Biblioteka Mat. 50, PWN, Warszawa, 1977 (in Polish); English transl.: World Sci., 1983.

[8] M. Stoll, *On the arithmetic of the curves* $y^2 = x^l + A$, *II*, J. Number Theory 93 (2002), 183–206.

Tomasz Jędrzejak
Institute of Mathematics
University of Szczecin
Wielkopolska 15
70-451 Szczecin, Poland
E-mail: tjedrzejak@gmail.com

Received April 22, 2008;
received in final form October 1, 2008 (7659)