Canad. Math. Bull. Vol. **50** (2), 2007 pp. 313–320

On Cauchy–Liouville–Mirimanoff Polynomials

Dedicated to the memory of John Isbell, 1930–2005

Pavlos Tzermias

Abstract. Let p be a prime greater than or equal to 17 and congruent to 2 modulo 3. We use results of Beukers and Helou on Cauchy–Liouville–Mirimanoff polynomials to show that the intersection of the Fermat curve of degree p with the line $X + Y = Z$ in the projective plane contains no algebraic points of degree d with $3 \leq d \leq 11$. We prove a result on the roots of these polynomials and show that, experimentally, they seem to satisfy the conditions of a mild extension of an irreducibility theorem of Pólya and Szegö. These conditions are *conjecturally* also necessary for irreducibility.

1 Introduction

Let $\mathbb{Q}$ be the field of rational numbers. For an integer $n \geq 2$, consider the polynomial $P_n(X) = (X+1)^n - X^n - 1$. The following identity is due to Cauchy and Liouville [4], [17, p. 46]:

$$P_n(X) = X(X+1)^a(X^2+X+1)^b E_n(X), \tag{1.1}$$

where $E_n(X) \in \mathbb{Z}[X]$ and a, b are defined as follows: if is n even, then $a = b = 0$, while if n is odd, then $a = 1$ and $b = 0, 1, 2$ according to whether $n \equiv 0, 2, 1 \pmod 3$, respectively. The polynomials $E_n(X)$ are called Cauchy–Liouville–Mirimanoff polynomials (in the literature, they are also referred to as Cauchy–Mirimanoff polynomials). For n prime, Mirimanoff [13] conjectured the irreducibility of $E_n(X)$ over $\mathbb{Q}$. It is not unlikely that $E_n(X)$ is in fact irreducible for all integers n. By a clever argument of Filaseta (described by Helou [9]), it is known that $E_{2p}(X)$ is irreducible over $\mathbb{Q}$ for all primes p. Analogous results for general n seem to be out of reach at the moment. Terjanian [19] has suggested an interesting generalization of Mirimanoff's original conjecture and Helou [8] has established an interesting connection with Wendt's binomial circulant determinant. The purpose of this paper is to prove the following result:

Theorem 1.1 *Let p be a prime such that $p \equiv 2 \pmod 3$ and $p \geq 17$.*

(i) *Every irreducible factor of $E_p(X)$ over $\mathbb{Q}$ is of degree $d \geq 12$.*
(ii) *For $p \geq 23$, $E_p(X)$ has an irreducible factor of degree $d \geq 18$.*

Received by the editors March 10, 2005; revised July 8, 2006.
AMS subject classification: Primary: 11G30, 11R09; secondary: 12D05, 12E10.

Part (i) of the above theorem strengthens a result of C. Robinson who, using a different method, showed the statement to be true for approximately 80% of such primes p. It can be restated in terms of low-degree points on Fermat curves (see also [5–7, 10–12, 16, 20–22].

Corollary 1.2 *Let p be a prime such that $p \geq 17$ and $p \equiv 2 \pmod 3$. If an algebraic point of degree $d \geq 3$ over $\mathbb{Q}$ belongs to the support of the intersection divisor of the Fermat curve $X^p + Y^p = Z^p$ with the line $X + Y = Z$ in $\mathbb{P}^2$, then $d \geq 12$.*

It appears that the polynomials $E_p(X)$ do not satisfy the conditions of most standard irreducibility criteria. In Section 3, we show that, experimentally, they seem to satisfy the conditions of a mild extension of an irreducibility theorem of Pólya and Szegö [15]. It is interesting to note that, at least for $p \equiv 2 \pmod 3$, the sufficient conditions for irreducibility of $E_p(X)$ provided by this theorem are *conjecturally* necessary conditions as well.

2 Low-Degree Factors

In this section, we prove Theorem1.1 by combining results of Helou [9] and Beukers [1]. Let n be odd such that $n \geq 9$. Helou [9] showed that the set of roots of $E_n(X)$ is partitioned into orbits of cardinality 6 under a natural action of S_3 and that the rational function

$$J(X) = \frac{(X^2 + X + 1)^3}{(X^2 + X)^2} \tag{2.1}$$

is invariant under the same action. Therefore, there exists a polynomial $T_n(X) \in \mathbb{Q}[X]$ of degree $r_n = (n - 3 - 2b)/6$ such that

$$E_n(X) = n(X^2 + X)^{2r_n} T_n(J(X)). \tag{2.2}$$

If $n = p$ is prime, it follows from Helou's work [9] that $T_p(X)$ is a monic polynomial with coefficients in $\mathbb{Z}$ whose roots are all real and simple and that $E_p(X)$ and $T_p(X)$ have the same number of irreducible factors over $\mathbb{Q}$. In particular, the degree d mentioned in Theorem 1.1 and Corollary 1.2 is always a multiple of 6. Now define

$$u = (X^2 + X + 1)^3, \quad v = (X^2 + X)^2. \tag{2.3}$$

It follows from (2.1), (2.2) and (2.3) that

$$E_n(X) = R_n(u, v), \tag{2.4}$$

where $R_n \in \mathbb{Z}[u, v]$ is a homogeneous polynomial in u, v of degree r_n. Also note that setting $T = J(X)$ we have

$$T_n(T) = \frac{1}{n} R_n(T, 1). \tag{2.5}$$

We have the following lemma.

https://doi.org/10.4153/CMB-2007-030-7 Published online by Cambridge University Press

Lemma 2.1 *For odd $n \geq 9$, the polynomials R_n satisfy the following recursive relation:*

$$R_{n+18}(u,v) = (2u+3v)R_{n+12}(u,v) + (6uv - u^2 - 3v^2)R_{n+6}(u,v) + v^3R_n(u,v).$$

Proof Observe that

$$((X+1)^6 + X^6)(P_{n+6}(X)+1) = P_{n+12}(X) + 1 + v^3(P_n(X)+1). \tag{2.6}$$

Since $(X+1)^6 + X^6 = 2u + 3v - 1$, the recursion follows from a straightforward calculation using (2.6) and the definitions of $E_n(X)$ and $R_n(u,v)$. ∎

We now discuss the roots of the polynomials T_n. As mentioned before, Helou has shown that all the roots of T_n are real and simple. We now prove that they are all negative:

Lemma 2.2 *For odd $n \geq 9$, all the roots of the polynomial T_n are negative. In particular, since T_n is monic, all its coefficients are positive.*

Proof By (2.5), it suffices to show that $R_n(T,1) > 0$ if $T \geq 0$. The first few polynomials $T_n(T)$ are listed below:

$$\begin{array}{lll} T_9(T) = T + \frac{1}{3} & T_{15}(T) = T^2 + \frac{10}{3}T + \frac{1}{5} & T_{21}(T) = T^3 + \frac{28}{3}T^2 + 7T + \frac{1}{7} \\ T_{11}(T) = T + 1 & T_{17}(T) = T^2 + 5T + 1 & T_{23}(T) = T^3 + 12T^2 + 14T + 1 \\ T_{13}(T) = T + 2 & T_{19}(T) = T^2 + 7T + 3 & T_{25}(T) = T^3 + 15T^2 + \frac{126}{5}T + 4. \end{array}$$

We distinguish two cases:

Case 1 Suppose $T > 6$. It clearly suffices to show that

$$R_{n+6}(T,1) > TR_n(T,1) > 0 \tag{2.7}$$

for all odd $n \geq 9$. It is straightforward to show that (2.7) is true for n in $\{9, 11, 13, 15, 17, 19\}$. Assume that (2.7) holds for all n such that $9 \leq n \leq 13 + 6k$, where $k \geq 1$. Let $c = 9, 11, 13$. Then by Lemma 2.1, our assumption on T and the induction hypothesis, we get

$$\begin{aligned} R_{c+6k+12}(T,1) &- TR_{c+6k+6}(T,1) \\ &= (T+3)R_{c+6k+6}(T,1) + (6T - T^2 - 3)R_{c+6k}(T,1) + R_{c+6k-6}(T,1) \\ &> (T^2+3T)R_{c+6k}(T,1) + (6T - T^2 - 3)R_{c+6k}(T,1) + R_{c+6k-6}(T,1) \\ &= (9T-3)R_{c+6k}(T,1) + R_{c+6k-6}(T,1) > 0, \end{aligned}$$

so (2.7) also holds for $n = c + 6(k+1)$.

Case 2 Suppose $0 \le T \le 6$. Since $R_9(T,1), R_{11}(T,1), R_{13}(T,1) > 0$, it suffices to show that

$$R_{n+12}(T,1) - R_{n+6}(T,1) \ge R_{n+6}(T,1) - R_n(T,1) \ge 0, \tag{2.8}$$

for all odd $n \ge 9$. It is straightforward to show that (2.8) holds for $n \in \{9, 11, 13\}$. Let $c = 9, 11, 13$. Suppose that (2.8) holds for $n = c + 6k$, where $k \ge 0$. Then by Lemma 2.1, our assumption on T and the induction hypothesis, we get

$$\begin{aligned}
R_{c+6k+18}&(T,1) - 2R_{c+6k+12}(T,1) + R_{c+6k+6}(T,1)\\
&= (2T+1)R_{c+6k+12}(T,1) + (6T - T^2 - 2)R_{c+6k+6}(T,1) + R_{c+6k}(T,1)\\
&= R_{c+6k+12}(T,1) - 2R_{c+6k+6}(T,1) + R_{c+6k}(T,1)\\
&\qquad + 2TR_{c+6k+12}(T,1) + T(6-T)R_{c+6k+6}(T,1)\\
&\ge R_{c+6k+12}(T,1) - 2R_{c+6k+6}(T,1) + R_{c+6k}(T,1) \ge 0,
\end{aligned}$$

so (2.8) holds for $n = c + 6(k+1)$.

∎

Proof of Theorem 1.1 As mentioned before, the work of Helou [9] implies that an irreducible factor of $E_p(X)$ over $\mathbb{Q}$ necessarily has degree d divisible by 6 and corresponds to an irreducible factor of $T_p(T)$ of degree $d/6$. So the proof of Theorem 1.1 reduces to the study of linear and quadratic factors of $T_p(T)$. By Lemma 2.1, the constant coefficient a_n of $T_n(T)$ satisfies the recursion

$$(n+18)a_{n+18} = 3(n+12)a_{n+12} - 3(n+6)a_{n+6} + na_n. \tag{2.9}$$

Now for $n \equiv -1 \pmod 6$, the initial conditions are $a_{11} = a_{17} = a_{23} = 1$. An easy inductive argument now shows that $a_n = 1$ for all $n \equiv -1 \pmod 6$. If, in addition, n is prime, then $T_n(T)$ is a monic polynomial with coefficients in $\mathbb{Z}$. Therefore, the only possible $\mathbb{Q}$-rational roots are 1 and -1. The former case is impossible by Lemma 2.2. To show that the latter case is also impossible, note that if -1 were a root of $T_n(T)$, then $T_{11}(T)$ would divide $T_n(T)$, which implies that $E_n(X)$ is divisible by $E_{11}(X)$. This is a contradiction, since, as Beukers shows in [1], the polynomials $E_n(X)$ are pairwise relatively prime. This proves part (i) of Theorem 1.1.

To prove part (ii), we need to show that there exists an irreducible factor of $T_p(T)$ of degree ≥ 3. Suppose this is not the case. Since $T_p(T)$ is a monic polynomial in $\mathbb{Z}[T]$ with constant term 1, it follows from Lemma 2.2 that $T_p(T)$ is the product of polynomials of the form $T+1$ and T^2+cT+1, with c a positive integer. In particular, $R_p(T,1)$ is a reciprocal polynomial. We show that this is impossible, unless $p = 11$ or 17. To do this, we use Lemma 2.1 to compare the coefficients of T^{r_p-1} and T in $R_n(T,1)$. Let c_n and d_n be the coefficients of T^{r_n-1} and T in $R_n(T,1)$, respectively (for $n \equiv -1 \pmod 6$). By Lemma 2.1 and the fact that the leading coefficient of $R_n(T,1)$ equals n, we get

$$c_{n+18} = 3n + 36 + 2c_{n+12} + 6n + 36 - c_{n+6} \tag{2.10}$$

with initial conditions $c_{11} = 11$, $c_{17} = 85$ and $c_{23} = 276$. By induction, we get

$$c_n = \frac{n(n-5)(n-7)}{24}. \tag{2.11}$$

To obtain a formula for d_n, we use Lemma 2.1 and differentiation at $T = 0$, taking into account that the constant term in $R_n(T, 1)$ equals n:

$$d_{n+18} = 2n + 24 + 3d_{n+12} + 6n + 36 - 3d_{n+6} + d_n \tag{2.12}$$

with initial conditions $d_{11} = 11$, $d_{17} = 85$ and $d_{23} = 322$. By induction, we get

$$d_n = \frac{n(n+1)(n-2)(n-5)}{648}. \tag{2.13}$$

Using (2.11) and (2.13), it is now easy to check that $c_n = d_n$ if and only if $n = 11$ or 17, and this completes the proof of Theorem 1.1. ■

3 An Irreducibility Criterion

We need the following mild extension of a classical theorem of Pólya and Szegö [15, vol. 2, VIII, 127]. We claim no novelty for the result whose proof is virtually identical to the proof of Pólya and Szegö's original theorem given in a paper by Brillhart, Filaseta and Odlyzko [3]:

Theorem 3.1 *If $f(X)$ is a polynomial in $\mathbb{Z}[X]$ of degree n with roots $\alpha_1, \dots, \alpha_n$ and there exists a rational number $\frac{r}{s}$ such that $s^n f(\frac{r}{s})$ is prime, $f(\frac{r}{s} - 1) \neq 0$ and $\operatorname{Re}(\alpha_i) < \frac{r}{s} - \frac{1}{2}$ for all $i \in \{1, \dots, n\}$, then $f(X)$ is irreducible in $\mathbb{Z}[X]$.*

Proposition 3.2 *Let p be a prime such that $p \geq 11$. Let $\frac{r}{s}$ be a rational number such that $\frac{r}{s} \geq \frac{1}{2}$. Suppose that $s^{r_p} T_p(\frac{r}{s})$ is a product of d primes (not necessarily distinct). Then $T_p(T)$ (and also $E_p(X)$) has at most d irreducible factors over $\mathbb{Q}$.*

Proof By Lemma 2.2 and the fact that $T_p(T) \in \mathbb{Z}[T]$ is monic, any rational root of $T_p(T)$ must be a negative integer. So if $T_p(\frac{r}{s} - 1) = 0$, then $\frac{r}{s} \leq 0$, a contradiction. Also, by Lemma 2.2, the inequality $\operatorname{Re}(\alpha_i) < \frac{r}{s} - \frac{1}{2}$ is satisfied for every root α_i of $T_p(T)$. Now by the proof of Theorem 3.1, for any irreducible factor $g(T)$ of $T_p(T)$ of degree k, we have $|s^k g(\frac{r}{s})| \geq 2$. Therefore, the number of irreducible factors of $T_p(T)$ cannot exceed the number of (not necessarily distinct) prime divisors of $s^{r_p} T_p(\frac{r}{s})$. ■

A few remarks are in order:

(1) By Proposition 3.2, the existence of a rational number $\frac{r}{s} \geq \frac{1}{2}$ such that $s^{r_p} T_p(\frac{r}{s})$ is prime implies that $E_p(X)$ is irreducible over $\mathbb{Q}$. Computationally, the existence of $\frac{r}{s}$ seems to be a frequent occurence. Table 1 lists such a rational $\frac{r}{s} \leq 1$ for each prime $p < 1000$. We should note that we list only one of several $\frac{r}{s}$ that our crude MAPLE program found for each prime p. Specifically, we list the first such rational number with respect to the lexicographic ordering of r, s. Each entry in the table is a triple (p, r, s).

(11,1,1)	(163,14,23)	(353,14,27)	(569,8,15)	(773,18,19)
(13,1,1)	(167,1,2)	(359,6,11)	(571,36,71)	(787,35,68)
(17,1,1)	(173,19,22)	(367,9,10)	(577,413,450)	(797,39,61)
(19,1,1)	(179,17,32)	(373,5,6)	(587,25,27)	(809,15,28)
(23,1,2)	(181,29,35)	(379,68,105)	(593,18,23)	(811,142,205)
(29,2,3)	(191,11,16)	(383,5,9)	(599,34,63)	(821,23,34)
(31,1,1)	(193,127,238)	(389,38,47)	(601,77,135)	(823,49,94)
(37,7,10)	(197,15,22)	(397,59,90)	(607,9,16)	(827,48,73)
(41,11,14)	(199,34,43)	(401,38,75)	(613,77,142)	(829,53,57)
(43,4,7)	(211,103,186)	(409,27,35)	(617,35,68)	(839,12,23)
(47,1,2)	(223,13,15)	(419,9,14)	(619,38,41)	(853,47,88)
(53,12,13)	(227,17,30)	(421,71,78)	(631,232,375)	(857,2,3)
(59,8,11)	(229,61,89)	(431,3,4)	(641,83,120)	(859,51,100)
(61,19,30)	(233,30,49)	(433,143,180)	(643,15,29)	(863,18,29)
(67,5,6)	(239,11,20)	(439,29,53)	(647,31,51)	(877,61,118)
(71,13,22)	(241,71,140)	(443,39,62)	(653,27,38)	(881,115,117)
(73,17,26)	(251,13,21)	(449,62,101)	(659,39,70)	(883,76,147)
(79,12,13)	(257,9,10)	(457,197,260)	(661,149,211)	(887,16,27)
(83,1,1)	(263,1,2)	(461,60,73)	(673,181,220)	(907,11,20)
(89,11,15)	(269,7,8)	(463,52,101)	(677,15,26)	(911,36,67)
(97,21,23)	(271,31,56)	(467,22,25)	(683,23,26)	(919,92,147)
(101,7,11)	(277,51,58)	(479,17,31)	(691,72,101)	(929,43,82)
(103,7,9)	(281,23,38)	(487,19,30)	(701,27,38)	(937,115,171)
(107,11,18)	(283,7,9)	(491,37,58)	(709,7,10)	(941,13,19)
(109,17,28)	(293,22,23)	(499,35,66)	(719,7,12)	(947,25,46)
(113,16,21)	(307,35,47)	(503,13,18)	(727,21,29)	(953,17,18)
(127,23,24)	(311,6,11)	(509,13,17)	(733,77,107)	(967,151,262)
(131,8,9)	(313,129,155)	(521,62,105)	(739,10,19)	(971,21,25)
(137,6,11)	(317,4,5)	(523,11,21)	(743,5,8)	(977,46,51)
(139,8,15)	(331,46,55)	(541,109,142)	(751,69,94)	(983,7,10)
(149,9,10)	(337,249,490)	(547,64,105)	(757,187,240)	(991,67,126)
(151,9,14)	(347,33,62)	(557,19,22)	(761,39,49)	(997,39,70)
(157,29,49)	(349,67,77)	(563,8,11)	(769,245,348)	

Table 1

(2) Numerical evidence suggests that the largest root of $T_p(T)$ approaches 0 as p approaches infinity. Consequently, it seems that the condition $\frac{r}{s} \geq \frac{1}{2}$ in Proposition 3.2 cannot be improved.

(3) It is interesting to note that the sufficient condition for irreducibility of $E_p(X)$ given by Proposition 3.2 is *conjecturally* a necessary condition as well, at least for $p \equiv 2 \pmod 3$. To be more specific, assume $T_p(T)$ is irreducible for a prime $p \equiv 2 \pmod 3$. One of the major unsolved problems in number theory is a famous conjecture of Bouniakowsky [2], which was rediscovered and generalized to polynomial systems in a paper of Schinzel and Sierpinski [18]. It asserts that for an irreducible polynomial $f(X) \in \mathbb{Z}[X]$ with positive leading coefficient, the set of values $V_f = \{f(n) : n \in \mathbb{Z}^+\}$ contains infinitely many primes, provided that the elements of V_f have no common prime divisor. We refer the reader to Murty's paper [14] for a discussion of the connection between prime numbers and irreducible polynomials as well as function field analogues of this connection. Replacing $f(X)$ by $g(X) = f(X-1)$, it is clear that we can replace $\mathbb{Z}^+$ by $\mathbb{Z}_+$ in the statement of Bouniakowsky's conjecture. Now note that $T_p(0) = 1$, so the elements of V_{T_p} have no common prime divisor. Therefore, Bouniakowsky's conjecture implies that $T_p(n)$ must be prime for infinitely many $n \in \mathbb{Z}_+$.

Acknowledgment I thank the anonymous referee for suggesting substantial improvements on the exposition.

References

[1] F. Beukers, *On a sequence of polynomials. Algorithms for algebra.* J. Pure Appl. Algebra **117/118**(1997), 97–103.

[2] V. Bouniakowsky, *Sur les diviseurs numériques invariables des fonctions rationelles entières.* Mémoires Sci. Math. Phys. **6** (1854-1855), 307–329.

[3] J. Brillhart, M. Filaseta and A. Odlyzko, *On an irreducibility theorem of A. Cohn.* Canad. J. Math. **33**(1981), no. 5, 1055–1059.

[4] A. Cauchy and J. Liouville, *Rapport sur un mémoire de M. Lamé relatif au dernier théoréme de Fermat.* C. R. Acad. Sci. Paris **9**(1839), 359–363.

[5] O. Debarre and M. Klassen, *Points of low degree on smooth plane curves.* J. Reine Angew. Math. **446**(1994), 81–87.

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

[7] B. Gross and D. Rohrlich, *Some results on the Mordell-Weil group of the Jacobian of the Fermat curve.* Invent. Math. **44**(1978), no. 3, 201–224.

[8] C. Helou, *On Wendt's determinant.* Math. Comp. **66**(1997) no. 219, 1341–1346.

[9] ———, *Cauchy-Mirimanoff polynomials.* C. R. Math. Rep. Acad. Sci. Canada **19**(1997), no. 2, 51–57.

[10] M. Klassen and P. Tzermias, *Algebraic points of low degree on the Fermat quintic.* Acta Arith. **82**(1997), no. 4, 393–401.

[11] W. McCallum, *The arithmetic of Fermat curves.* Math. Ann. **294**(1992), no. 3, 503–511.

[12] W. McCallum and P. Tzermias, *On Shafarevich-Tate groups and the arithmetic of Fermat curves.* In: Number Theory and Algebraic Geometry. London Math. Soc. Lecture Note Ser. 303, Cambridge University Press, Cambridge, 2003, pp. 203–226.

[13] D. Mirimanoff, *Sur l'équation* $(x+1)^l - x^l - 1 = 0$. Nouv. Ann. Math. **3**(1903), 385–397.

[14] M. Ram Murty, *Prime numbers and irreducible polynomials.* Amer. Math. Monthly **109**(2002), no. 5, 452–458.

[15] G. Pólya and G. Szegö, *Aufgaben und Lehrsätze aus der Analysis.* Springer-Verlag, Berlin, 1964.

[16] P. Ribenboim, *Homework!.* In: Number Theory. CRM Proc. Lecture Notes 19, American Mathematical Socoety, Providence, RI, 1999, pp. 391–392.

[17] ———, *13 Lectures on Fermat's Last Theorem.* Springer-Verlag, New York, 1979.

[18] A. Schinzel and W. Sierpinski, *Sur certaines hypothèses concernant les nombres premiers.* Acta Arith. **4**(1958), 185–208; Erratum, ibid. **5**(1958) 259.
[19] G. Terjanian, *Sur la loi de réciprocité des puissances l-émes.* Acta Arith. **54**(1989), no. 2, 87–125.
[20] P. Tzermias, *Low-degree points on Hurwitz-Klein curves.* Trans. Amer. Math. Soc. **356**(2004), no. 3, 939–951.
[21] ———, *Parametrization of low-degree points on a Fermat curve.* Acta Arith. **108**(2003), no. 1, 25–35.
[22] ———, *Algebraic points of low degree on the Fermat curve of degree seven.* Manuscripta Math. **97**(1998), no. 4, 483–488.

Department of Mathematics
University of Tennessee
Knoxville, TN 37996-1300
U.S.A.
e-mail: tzermias@math.utk.edu