J. Aust. Math. Soc. **92** (2012), 269–280
doi:10.1017/S1446788712000195

CAUCHY–MIRIMANOFF AND RELATED POLYNOMIALS

PAUL M. NANNINGA

(Received 30 April 2011; accepted 1 February 2012)

Communicated by I. E. Shparlinski

Dedicated to the memory of Alf van der Poorten

Abstract

In 1903 Mirimanoff conjectured that Cauchy–Mirimanoff polynomials E_n are irreducible over $\mathbb{Q}$ for odd prime n. Polynomials R_n, S_n, T_n are introduced, closely related to E_n. It is proved that R_m, S_m, T_m are irreducible over $\mathbb{Q}$ for odd $m \geq 3$, and E_n, R_n, S_n are irreducible over $\mathbb{Q}$, for $n = 2^q m$, $q = 1, 2, 3, 4, 5$, and $m \geq 1$ odd.

2010 *Mathematics subject classification*: primary 11C08.

Keywords and phrases: irreducible polynomials, Cauchy–Mirimanoff polynomial, Fermat's last theorem.

1. Introduction

The study of Cauchy–Mirimanoff polynomials E_n was initiated by Cauchy and Liouville [2] in 1839 in the context of Fermat's last theorem. In 1903 Mirimanoff [6] conjectured that E_p is irreducible over $\mathbb{Q}$ for any odd prime p. Little progress was made on this subject for more than 90 years, until Helou [3] investigated the Galois group of E_n. Helou showed that for odd $n \geq 9$, the roots of E_n occur in sets of six (corresponding to the six automorphisms of E_n), and all of the roots of any factor polynomial also occur in sets of six. In the same paper Helou gave a proof, credited to M. Filaseta, based on the Newton polygon of E_n, that E_{2p} is irreducible over $\mathbb{Q}$ for any odd prime p. In 1997 Beukers [1] proved that the E_p are relatively prime to each other. In 2007, Tzermias [10] proved a necessary condition for the irreducibility of polynomials over $\mathbb{Q}$ (an extension of Pólya and Szegő's irreducibility theorem) and used this to prove that E_p is irreducible over $\mathbb{Q}$ for any prime $p < 1000$. Tzermias stated that 'It is not unlikely that E_n is irreducible for all integers n'. In 2010 Irick [4] gave a proof of the irreducibility of E_{2p} (different from Filaseta's), proved that E_{3p} is irreducible, and investigated the irreducibility of E_{3p^i}. Other authors have demonstrated properties of the Cauchy–Mirimanoff polynomials, including Klösgen [5] and Terjanian [9]. A bibliography of Ribenboim [7, pp. 231–234] lists several more.

In this paper polynomials $R_n, S_n, T_n \in \mathbb{Z}[x]$, close relatives of E_n, are introduced. These polynomials have even degree, and all of their coefficients are positive. It is shown here that all of their roots are simple and lie in the open strip $-1 < \mathrm{Re}(z) < 0$, that none of the roots are real, and that the polynomials and all of their factors in $\mathbb{Z}[x]$ are Hurwitz stable. It is proved that R_m, S_m, T_m are irreducible over $\mathbb{Q}$ for odd $m \geq 3$, and E_n, R_n, S_n are irreducible over $\mathbb{Q}$, for $n = 2^q m$, where $q = 1, 2, 3, 4, 5$ and $m \geq 1$ is odd. It is conjectured that E_n, R_n, S_n, and T_n are irreducible over $\mathbb{Q}$ for $n \geq 2$.

2. The polynomials E_n, R_n, S_n and T_n

We define $E_n, R_n, S_n, T_n \in \mathbb{Z}[x]$ as follows.

(1) For $n \geq 2$, $(x+1)^n - x^n - 1 = x(x+1)^a(x^2+x+1)^b E_n$, where $a = b = 0$ if n is even; while if n is odd, $a = 1$ and $b = 0, 1, 2$ according as $n \equiv 3, -1, 1 \bmod 6$ (Helou [3]).

(2) For $n \geq 1$, $(x+1)^n + x^n - 1 = x(x+1)^a R_n$, where $a = 0$ if n is odd, and $a = 1$ if n is even.

(3) For $n \geq 1$, $(x+1)^n - x^n + 1 = (x+1)^a S_n$, where $a = 0$ if n is odd and $a = 1$ if n is even.

(4) For $n \geq 1$, $(x+1)^n + x^n + 1 = (x+1)^a(x^2+x+1)^b T_n$, where $a = 1$ and $b = 0$ if n is odd; while if n is even, $a = 0$ and $b = 0, 1, 2$ according as $n \equiv 0, 2, -2 \bmod 6$.

The coefficients of E_n, R_n, S_n and T_n can be obtained by using the binomial expansion in their definitions. The following explicit formulae will be used in this paper.

(1) If $n \geq 2$ is even, then $R_n = \sum_{i=0}^{n-2} \alpha_i x^i$, where

$$\alpha_i = (-1)^i \sum_{j=0}^{i} (-1)^j \binom{n}{j+1} \quad \text{for } i = 0, \ldots, n-2. \tag{1}$$

(2) If $n \geq 1$ is odd, then $R_n = \sum_{i=0}^{n-2} \alpha_i x^i + 2x^{n-1}$, where

$$\alpha_i = \binom{n}{i+1} \quad \text{for } i = 0, \ldots, n-2. \tag{2}$$

(3) If $n \geq 2$ is even, then $E_n = \sum_{i=0}^{n-2} \alpha_i x^i$, where

$$\alpha_i = \binom{n}{i+1} \quad \text{for } i = 0, \ldots, n-2.$$

https://doi.org/10.1017/S1446788712000195 Published online by Cambridge University Press

To show the relationships between the polynomials E_n, R_n, S_n, and T_n, it is convenient to define the following matrices $A_i \in \mathrm{GL}_2(\mathbb{Z})$:

$$\begin{aligned} A_1 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \\ A_4 &= \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \quad A_5 = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}, \quad A_6 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}. \end{aligned} \tag{3}$$

For any $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, define the action of A on $\mathbb{Z}[x]$ by mapping $f \in \mathbb{Z}[x]$ to $f^A(x) = (cx+d)^{d_n} f((ax+b)/(cx+d))$, where $d_n = \deg f$. Then from the definition of T_n for even $n \geq 2$,

$$T_n = T_n^{A_2} = T_n^{A_3} = T_n^{A_4} = T_n^{A_5} = T_n^{A_6},$$

and exactly the same formulae hold for E_n for odd $n \geq 3$. For odd $n \geq 1$,

$$T_n = T_n^{A_2}.$$

For even $n \geq 2$, E_n, R_n, S_n are related by

$$R_n = R_n^{A_3}, \tag{4}$$
$$R_n = E_n^{A_6}, \tag{5}$$
$$R_n = S_n^{A_2}, \tag{6}$$
$$S_n = S_n^{A_5},$$
$$S_n = E_n^{A_3}. \tag{7}$$

For odd $n \geq 1$, R_n, S_n and T_n are related by

$$R_n = R_n^{A_5}, \tag{8}$$
$$R_n = T_n^{A_3}, \tag{9}$$
$$S_n = S_n^{A_3},$$
$$S_n = R_n^{A_2}. \tag{10}$$

Lemma 1. *E_n, R_n, S_n and T_n have no real roots.*

Proof. From their definitions the polynomials E_n, R_n, S_n and T_n can only have roots for $n \geq 3$. Begin with R_n. First we show that 0 and -1 are not roots of R_n. From the definition of R_n and the binomial expansion,

$$(x+1)^a R_n(x) = \sum_{i=0}^{n-2} \binom{n}{i+1} x^i + 2x^{n-1},$$

so that $R_n(0) = n \geq 3$, that is, $x = 0$ is not a root of R_n for any n. By (4), for even n, $R_n(-1) = R_n(0) \neq 0$. For odd n, $xR_n(x) = (x+1)^n + x^n - 1$ and consequently $R_n(-1) = 2$, so -1 is not a root of R_n for odd n either.

Now suppose that $x \in \mathbb{R} \setminus \{0, -1\}$ is a root of R_n. From the definition of R_n, x satisfies $(x+1)^n + x^n = 1$, so that $x > 0$ is clearly impossible. If $-1 < x < 0$ then for $n \geq 2$, $1 = |(x+1)^n + x^n| \leq |x+1|^n + |x|^n < |x+1| + |x| = 1$, a contradiction. For $x < -1$ replace x by $-y-1$ with $y > 0$ so that $(y+1)^n + y^n = \pm 1$, depending on the parity of n. Both cases give a contradiction. Therefore, R_n has no real roots.

By (10) and (6), S_n has no real roots because R_n has none. Similarly, by (9), T_n has no real roots for odd n, and by (5), E_n has no real roots for even n. A proof that E_n has no real roots for $n = 6k \pm 1$ is given by Ribenboim [7, pp. 223–225]. For odd n it remains to prove there are no real roots for $n = 6k+3$. In this case the symmetries $E_n(x) = x^{d_n} E_n(1/x)$ and $E_n(x) = E_n(-x-1)$ apply, and so Ribenboim's proof also applies to $n = 6k+3$. Finally, consider the roots of T_n for n even. But there can be no real root in this case as for all $x \in \mathbb{R}$, $(x+1)^n + x^n + 1 > 1$. $\square$

Lemma 2. *All of the roots of E_n, R_n, S_n and T_n lie in the open strip $-1 < \mathrm{Re}(z) < 0$.*

Proof. The polynomials E_n, R_n, S_n and T_n are constant for $n \leq 2$, so assume that $n \geq 3$. Let $P_n(e, f; x) = (x+1)^n + ex^n + f \in \mathbb{Z}[x]$, where $e, f \in \{1, -1\}$. For appropriate choices of e, f, each of the polynomials E_n, R_n, S_n and T_n is a factor of P_n over $\mathbb{Z}$. Note that if z is a root of P_n, then $|(z+1)^n + ez^n| = 1$. Let $z = a + ib \neq 0, -1$, with $a, b \in \mathbb{R}$, be a root of P_n, so that $|(a+1+ib)^n + e(a+ib)^n| = 1$. By the (inverse) triangle inequality, if z_1, z_2 are any two complex numbers, then $|z_1 + z_2| \geq ||z_1| - |z_2||$. In this inequality select $z_1 = (a+1+ib)^n$ and $z_2 = e(a+ib)^n$, so that $1 \geq |((a+1)^2 + b^2)^{n/2} - (a^2+b^2)^{n/2}|$.

But if $a \geq 0$ (note that $b \neq 0$ if $a = 0$ because it is assumed that $z \neq 0$), then $|((a+1)^2 + b^2)^{n/2} - (a^2+b^2)^{n/2}| = ((a+1)^2 + b^2)^{n/2} - (a^2+b^2)^{n/2} > 1$, for $n \geq 3$. This contradicts the earlier inequality, so it follows that $a < 0$ if $n \geq 3$.

Now note that $P_n(e, f; -x-1) = (-x)^n + e(-x-1)^n + f = (-1)^n e P_n(e, ef(-1)^n; x)$. Therefore, the previous argument demonstrating the impossibility of $a \geq 0$ also works for $a \leq -1$, and it follows that $-1 < a < 0$. That is, if $n \geq 3$, all of the roots of P_n must lie in the open strip $-1 < \mathrm{Re}(z) < 0$, with the possible exception of $z = 0$, $z = -1$.

Even if $z = 0$, $z = -1$ are roots of P_n, they cannot be roots of E_n, R_n, S_n or T_n because these polynomials have no real roots (Lemma 1). Then from their definitions E_n, R_n, S_n and T_n share the same roots as P_n (for appropriate values of e and f) with the only exceptions being $z = 0$, $z = -1$, and possibly the roots of $z^2 + z + 1$, but the latter lie in $-1 < \mathrm{Re}(z) < 0$ anyway. $\square$

Definition 3. A Hurwitz (or Hurwitz stable) polynomial $H \in \mathbb{R}[x]$ is defined by the property that all of its roots have negative real part.

Note that a Hurwitz polynomial is sometimes defined to have all of its coefficients the same sign, but Lemma 4 below shows that this is a consequence of the property given in the above definition. Also, for a polynomial to have all of its coefficients the same sign is not sufficient for the Hurwitz property to apply, for example $H(x) = x^3 + x^2 + 4x + 30$ has roots $1 \pm 3i$.

https://doi.org/10.1017/S1446788712000195 Published online by Cambridge University Press

Lemma 4. *All of the coefficients of any Hurwitz polynomial H, have the same sign. Every factor of H over $\mathbb{Z}$ is Hurwitz.*

Proof. By definition $H \in \mathbb{R}[x]$ and all of its roots have negative real part. Let H have leading coefficient $a_n(\neq 0) \in \mathbb{R}$, so it is enough to consider the monic polynomial $P = H/a_n$. Now P can be factored into linear factors $x + r$ corresponding to the real roots of P, and quadratic factors $(x + c)(x + \bar{c}) = x^2 + ax + b$ corresponding to the complex roots. The real numbers r, a, b are positive because every root has negative real part. Therefore all of the coefficients of P are positive, and so all of the coefficients of H have the same sign. Also, all of the roots of any factor $g \in \mathbb{Z}[x]$ of H must also belong to H, so by definition g is also Hurwitz. □

Corollary 5. *E_n, R_n, S_n and T_n are Hurwitz polynomials. All of their coefficients are positive, and each of their factors in $\mathbb{Z}[x]$ are Hurwitz polynomials of even degree. All of the coefficients of each of these polynomials have the same sign.*

Proof. From their definitions E_n, R_n, S_n and T_n have positive leading coefficients, and by Lemma 2 all of their roots have negative real part. Then, by definition, these polynomials are Hurwitz. It follows from Lemma 4 that all of their factors in $\mathbb{Z}[x]$ are Hurwitz, and all of the coefficients of any such factor have the same sign. From Lemma 1 all of the roots of E_n, R_n, S_n and T_n occur in conjugate pairs, and since any pair belongs to the same polynomial, each factor of E_n, R_n, S_n and T_n over $\mathbb{Z}$ must have even degree. □

Lemma 6. *All of the roots of E_n, R_n, S_n and T_n are simple.*

Proof. From their definitions each of the polynomials E_n, R_n, S_n and T_n is a factor (over $\mathbb{Z}$) of $P_n(e, f; x) = (x + 1)^n + ex^n + f$, for appropriate values of $e, f \in \{1, -1\}$. Assume that $P_n(e, f; x)$ has a complex root z, with non-zero imaginary part (none of the roots of E_n, R_n, S_n and T_n are real by Lemma 1) and of multiplicity at least 2. Then $P_n(e, f; z) = 0$ and $P_n'(e, f; z) = 0$, where a prime denotes the derivative. Then $(z + 1)^n + ez^n + f = 0$ and $(z + 1)^{n-1} + ez^{n-1} = 0$. Multiplying the second of these equations by $z + 1$ and subtracting the result from the first equation gives $z^{n-1} = f/e = \pm 1$. Substituting this into the second equation gives $(z + 1)^{n-1} = -f = \pm 1$. Therefore z and $z + 1$ are complex $(n - 1)$th roots of ± 1, and $|z| = |z + 1| = |1 + 1/z| = 1$. These last conditions require that $z = -(1 \pm \sqrt{-3})/2$, so that $z^3 = 1$ and $(z + 1)^3 = -1$. Then $z^{n-1} = f/e$ implies that $n = 3j + 1$ for some integer j with $e = f$, and $(z + 1)^{n-1} = -f$ implies that $f = (-1)^{j+1}$. The requirement that $e = f$ immediately implies that R_n and S_n (for which $e \neq f$) must have only simple roots. In the case of E_n, $e = f = -1$ so that $f = (-1)^{j+1}$ implies that j must be even, that is, $n = 6k + 1$ for integer k. It is proved by Ribenboim [7, pp. 220–221] that $g = x^2 + x + 1$ does not divide E_n for any $n = 6k \pm 1$ and therefore $z = -(1 \pm \sqrt{-3})/2$, which are the roots of g, cannot be roots of E_n. Therefore E_n has only simple roots. The final case to consider is $e = f = 1$, which corresponds to T_n. In this case j is odd so that $n = 6k - 2$ for integer k. By the definition of T_n for $n = 6k - 2$, $P_n(1, 1; x) = g(x)^2 T_n(x)$. If $z = -(1 \pm \sqrt{-3})/2$

are roots of T_n, then g must be a factor of T_n and so z must have multiplicity at least 3 in $P_n(1, 1; x)$. Then $P''_n(1, 1; z) = 0$, which gives $(z + 1)^{n-2} + z^{n-2} = 0$. Multiplying by $z + 1$ gives $(z + 1)^{n-1} + z^{n-1} + z^{n-2} = 0$, and also $(z + 1)^{n-1} + z^{n-1} = 0$ from $P'_n(1, 1; z) = 0$. Subtraction gives $z^{n-2} = 0$, which is impossible. Therefore T_n has only simple roots. □

Before investigating the irreducibility of E_n, R_n, S_n and T_n in the next section, some simple polynomial properties need to be established. In the following $\mathrm{cont}(f)$, the content of $f \in \mathbb{Z}[x]$, is the gcd of all of the coefficients of f.

Lemma 7. *If $A \in \mathrm{GL}_2(\mathbb{Z})$ and $f \in \mathbb{Z}[x]$, then $\mathrm{cont}(f) = \mathrm{cont}(f^A)$, and f is irreducible over $\mathbb{Z}$ if and only if f^A is irreducible over $\mathbb{Z}$.*

Lemma 8. *Let $f \in \mathbb{Z}[x]$, with $\lambda = \mathrm{cont}(f)$, be such that $f^A = \pm f$, where $A \in \mathrm{GL}_2(\mathbb{Z})$. Assume that f is not proportional to a pure power of an irreducible polynomial in $\mathbb{Z}[x]$. Then either:*

(1) *there exist distinct primitive polynomials $g_1, g_2 \in \mathbb{Z}[x]$, with degree at least 1, such that $f = \pm\lambda g_1 g_2$, with $g_1^A = \pm g_1$ and $g_2^A = \pm g_2$; or*

(2) *there exist an integer $k \geq 2$ and distinct primitive polynomials $g_i \in \mathbb{Z}[x]$ for $i = 1, \ldots, k$, all with the same degree (at least 1), such that $f = \pm\lambda g_1 \cdots g_k$, with $g_i^A = g_{i+1}$ for $i = 1, \ldots, k-1$ and $g_k^A = \pm g_1$. Also, every g_i is the same pure power of an irreducible polynomial in $\mathbb{Z}[x]$.*

Proof. Write f as a product of distinct primitive polynomials $f = \lambda F_1 \cdots F_N$ where $F_i = f_i^{n_i}$ and each $f_i \in \mathbb{Z}[x]$ is distinct, primitive and irreducible over $\mathbb{Z}$ (with degree at least 1). Then F_i^A is a distinct primitive factor of f^A, and hence of f. So the action of A permutes the factors F_i of f (with a possible sign change). Since $\det A = \pm 1$ the action A has an inverse, so it generates the action of a cyclic group on $\mathbb{Z}[x]$. The F_i form orbits under this action. Let $G_i \in \mathbb{Z}[x]$ be the product of such elements (including F_i) in one such orbit, that is, $G_i = F_i \cdot F_i^A \cdot F_i^{A^2} \cdots F_i^{A^{k_i-1}}$, where $k_i \geq 1$ is the length of the orbit. Then G_i is a pure power of a primitive polynomial with the property that $G_i^A = \pm G_i$, and each G_i is distinct. It follows that if f has at least two orbits (so $\deg f \geq 2$) then there exist distinct primitive polynomials $g_1, g_2 \in \mathbb{Z}[x]$ of degree at least 1 (g_1, g_2 are products, not necessarily unique, of the polynomials G_i) such that $f = \pm\lambda g_1 g_2$, where $g_1^A = \pm g_1$ and $g_2^A = \pm g_2$.

If f has only one orbit (so f is proportional to a pure power of a product of distinct, primitive and irreducible polynomials all with the same degree), then $f = \pm\lambda F \cdot F^A \cdot F^{A^2} \cdots F^{A^{k-1}}$, where F is a pure power of a primitive irreducible polynomial in $\mathbb{Z}[x]$ (of degree at least 1), and $k \geq 1$ is the length of the orbit. The special case of a single orbit of length $k = 1$ is excluded by an assumption of the lemma, because it corresponds to f being proportional to a pure power of an irreducible polynomial. For a single orbit of length $k \geq 2$, set $g_i = F^{A^{i-1}}$ for $i = 1, \ldots, k$. Then each distinct g_i is a pure power of a primitive irreducible polynomial with the property that $g_i^A = g_{i+1}$ for $i = 1, \ldots, k-1$ and $g_k^A = \pm g_1$. □

Corollary 9. *If $A^2 = I_2$ and $A \neq \pm I_2$, then take $k = 2$ and $g_2^A = g_1$ in Lemma 8.*

Proof. Assuming that Lemma 8 applies to f, and that f has only one orbit with respect to A, then its length is $k \geq 2$. In the proof of the lemma $g_i = F^{A^{i-1}}$ for $i = 1, \ldots, k$. If $A^2 = I_2$ then $g_2^A = F^{A^2} = F = g_1$, and since $A \neq \pm I_2$ the length of the orbit can be taken to be $k = 2$. □

Note that the A_i defined by Equations (3) satisfy $A_2^2 = A_3^2 = A_5^2 = I_2$ so that the Corollary can be applied to these cases.

3. Irreducibility of E_n, R_n, S_n, T_n

In this section it is proved that R_m, S_m, T_m are irreducible over $\mathbb{Q}$ for odd $m \geq 3$ (Theorem 10), and E_n, R_n, S_n are irreducible over $\mathbb{Q}$, for $n = 2^q m$, $q = 1, 2, 3, 4, 5$, and $m \geq 1$ odd (Theorem 15). It is conjectured that E_n, R_n, S_n, T_n are irreducible over $\mathbb{Q}$ for all values of $n \geq 2$.

As mentioned in the introduction, Filaseta proved that for any odd prime p, E_{2p} is irreducible over $\mathbb{Q}$ (this appears to be the first proof that E_n is irreducible over $\mathbb{Q}$ for an infinite number of values of n). For even n, according to (5) and (7) respectively, $R_n = E_n^{A_6}$ and $S_n = E_n^{A_3}$. It follows from Lemma 7 that R_{2p} and S_{2p} are irreducible over $\mathbb{Q}$. Also, by (2), if p is any odd prime,

$$R_p(x) = \sum_{i=0}^{p-2} \binom{p}{i+1} x^i + 2x^{p-1}.$$

Then R_p is irreducible over $\mathbb{Q}$ by the Eisenstein irreducibility criterion (Stewart and Tall [8, p. 19]). For odd n, according to (10) and (9) respectively, $S_n = R_n^{A_2}$ and $R_n = T_n^{A_3}$, and it follows from Lemma 7 that S_p and T_p are irreducible over $\mathbb{Q}$. Theorems 10 and 15 extend all of these results.

Theorem 10. *R_n, S_n and T_n are irreducible over $\mathbb{Q}$ for odd $n \geq 3$.*

Proof. Suppose that n is odd, so that R_n is primitive (leading coefficient 2, odd constant coefficient), and $R_n(x) = (x+1)^{n-1} R_n(-x/(x+1))$ by (8). Also, by Lemma 6, R_n has only simple roots so it cannot be proportional to a power (at least 2) of an irreducible polynomial in $\mathbb{Z}[x]$. Assume now that R_n is reducible over $\mathbb{Q}$ (and therefore over $\mathbb{Z}$ by the Gauss polynomial lemma). Corollary 9 can be applied to R_n with $A = A_5$ (note that the content $\lambda = 1$ because R_n is primitive). From Lemma 8 there exist primitive relatively prime polynomials $g_1, g_2 \in \mathbb{Z}[x]$, of degree $r \geq 1$ and $s \geq 1$ respectively, such that $R_n = g_1 g_2$, with either:

(1) $g_1(x) = (x+1)^r g_1(-x/(x+1))$ and $g_2(x) = (x+1)^s g_2(-x/(x+1))$; or
(2) $g_1(x) = (x+1)^s g_2(-x/(x+1))$ and $g_2(x) = (x+1)^r g_1(-x/(x+1))$.

Note that the signs have been dropped by applying Corollary 5, and r, s are even (so $r, s \geq 2$) with $r = s$ in case (2).

https://doi.org/10.1017/S1446788712000195 Published online by Cambridge University Press

Set $g_1(x) = a_r x^r + \cdots + a_0$ and $g_2(x) = b_s x^s + \cdots + b_0$, where all $a_i, b_j \in \mathbb{Z}^+$ by Corollary 5. The leading coefficient of R_n is 2 so that $a_r b_s = 2$. In case (1), $g_1(1) = 2^r g_1(-1/2) = a_r(-1)^r + 2a_{r-1}(-1)^{r-1} + \cdots + 2^r a_0$ and $g_2(1) = 2^s g_2(-1/2) = b_s(-1)^s + 2b_{s-1}(-1)^{s-1} + \cdots + 2^s b_0$. In case (2), $g_1(1) = 2^s g_2(-1/2) = b_s(-1)^s + 2b_{s-1}(-1)^{s-1} + \cdots + 2^s b_0$ and $g_2(1) = 2^r g_1(-1/2) = a_r(-1)^r + 2a_{r-1}(-1)^{r-1} + \cdots + 2^r a_0$ (with $r = s$).

Since one of a_r, b_s must be 1, and the other 2, in both cases one of $g_1(1), g_2(1)$ must be odd and the other even. But from the definition of R_n, $R_n(1) = 2^n = g_1(1)g_2(1)$, so that one of $g_1(1), g_2(1)$ must be 1. Since g_1, g_2 both have degree at least 2, and all of their coefficients are positive, it follows that $g_1(1) > 1$ and $g_2(1) > 1$, a contradiction. Therefore, for odd n, R_n is irreducible over $\mathbb{Q}$. According to (10) and (9) respectively, $S_n = R_n^{A_2}$ and $R_n = T_n^{A_3}$, and it follows from Lemma 7 that S_n and T_n are irreducible over $\mathbb{Q}$. □

Lemma 11. *Let p be any prime, let $J, K \in \mathbb{Z}^+$ be such that $K \le p - 1$, and assume that J is not divisible by p. Let $r \ge s \ge 0$ be any integers such that $Kp^r \ge Jp^s$. If $v_p(x)$ is the p-adic valuation of x, then*

$$v_p\left(\binom{Kp^r}{Jp^s}\right) = r - s.$$

Proof. For any prime p and positive integers n, m, a theorem of Kummer (Ribenboim [7, pp. 75–77]) can be put into the form $v_p(\binom{n}{m}) = N$, for $n \ge m$, where N is the number of integers $j \ge 0$ for which $\{m/p^j\} > \{n/p^j\}$, where $\{x\}$ denotes the fractional part of a real number x. Setting $n = Kp^r$ and $m = Jp^s$, then N is the number of integers $j \ge 0$ for which $\{Jp^{s-j}\} > \{Kp^{r-j}\}$. For $j = 0, \ldots, s$ the inequality is not satisfied as both sides are zero. Since, by assumption, p does not divide J, K, the inequality is satisfied for $j = s + 1, \ldots, r$ because then $\{Jp^{s-j}\} > 0$ while $\{Kp^{r-j}\} = 0$. For $j > r$, $\{Kp^{r-j}\} \ge \{Jp^{s-j}\}$ as $0 < Kp^{r-j} < 1$ (because it is assumed that $K \le p - 1$) so that $\{Kp^{r-j}\} = Kp^{r-j}$, and $Kp^r \ge Jp^s$ by assumption. Therefore $N = r - s$. □

Lemma 12. *Let $n = 2^q m$ with $q \ge 1 \in \mathbb{Z}$ and odd $m \ge 1$, and let $i \in \mathbb{Z}$ be such that $0 \le i \le 2^q - 2$. Then*

$$v_2\left(\binom{n}{i+1}\right) = q - t, \tag{11}$$

where $i = 2^t N - 1$, $t \ge 0$ and $N \ge 1$ is odd. Consequently,

$$v_2\left(\binom{n}{i+1}\right) \begin{cases} = q - t + 1 & \text{if } i = 2^{t-1} - 1, \\ > q - t + 1 & \text{if } 2^{t-1} - 1 < i \le 2^t - 2. \end{cases} \tag{12}$$

Proof. First note that for any integers a, b with $a, b \ne 0$,

$$v_2(a \pm b) \begin{cases} = \min(v_2(a), v_2(b)) & \text{if } v_2(a) \ne v_2(b) \\ \ge v_2(a) + 1 & \text{if } v_2(a) = v_2(b). \end{cases} \tag{13}$$

Also, $v_2(a/b) = v_2(a) - v_2(b)$ and $v_2(ab) = v_2(a) + v_2(b)$. Suppose that $0 \le i \le 2^q - 2$, and let $k \in \mathbb{Z}$ such that $0 < k \le i$. Then $v_2(k) < q = v_2(n)$ so that $v_2((n-k)/k) = v_2(n-k) - v_2(k) = 0$ by (13). Taking the 2-adic valuation of

$$\binom{n}{i+1} = (n/(i+1)) \prod_{k=1}^{i} ((n-k)/k)$$

gives

$$v_2\left(\binom{n}{i+1}\right) = v_2(n/(i+1)) + \sum_{k=1}^{i} v_2((n-k)/k) = q - v_2(i+1).$$

There exist unique $t, N \in \mathbb{Z}$ such that $i = 2^t N - 1$ with $N \ge 1$ odd and $t \ge 0$, and since $i \le 2^q - 2$ it follows that $t \le q - \log_2(N) \le q$. Then $v_2(i+1) = t$ and (11) is proved. In particular, replacing t by $t-1$, and putting $N = 1$ so that $i = 2^{t-1} - 1$, then $v_2(\binom{n}{i+1}) = q - t + 1$ by (11); this is the first case of (12). If $i = 2^{t_0} N - 1$ for some odd $N \ge 1$ and integer $t_0 \ge 0$ such that $2^{t-1} - 1 < i \le 2^t - 2$, then $2^{t_0} \le (2^t - 1)/N < 2^t$, so $t_0 < t$. But if $t_0 = t - 1$ then $2^{t-1} < 2^{t-1} N \le 2^t - 1$, so $N \ge 2$ by the left inequality. But then the right-hand inequality $2^{t-1} N \le 2^t - 1$ is impossible. Therefore $t_0 < t - 1$ and $v_2(\binom{n}{i+1}) = q - t_0 > q - t + 1$, the second case of (12). □

Lemma 13. *Let $n = 2^q m$ with $q \ge 1$ and $m \ge 1$ odd. Write $R_n(x) = \sum_{i=0}^{n-2} \alpha_i x^i$ with α_i given by Equation (1). Then*

$$v_2(\alpha_i) = q - t + 1 \quad \text{for } 2^{t-1} - 1 \le i \le 2^t - 2, t = 1, \ldots, q, \tag{14}$$

and consequently $v_2(\alpha_i) \le v_2(\alpha_{i-1})$ for $i = 1, \ldots, 2^q - 2$. In particular, if $n = 2^q$ then the 2-adic valuations of all of the α_i are obtained from (14).

Proof. From equation (1),

$$\alpha_i = \binom{n}{i+1} - \alpha_{i-1}, \quad i = 1, \ldots, n-2. \tag{15}$$

Proceed by induction on t. Clearly (14) is true for $t = 1$ as $\alpha_0 = 2^q m$. Assume that (14) is true for some $q > t \ge 1$, so in particular $v_2(\alpha_{i_0}) = q - t + 1$ for $i_0 = 2^t - 2$. Let $i_1 = i_0 + 1 = 2^t - 1$. Then replacing t by $t + 1$ in (12), $v_2(\binom{n}{i_1+1}) = q - (t+1) + 1 = q - t$. From (15), $\alpha_{i_1} = (\binom{n}{i_1+1}) - \alpha_{i_0}$, and taking the 2-adic valuation using (13),

$$v_2(\alpha_{i_1}) = \min\left(v_2\left(\binom{n}{i_1+1}\right), v_2(\alpha_{i_0})\right) = \min(q-t, q-t+1) = q - t.$$

So (14) is confirmed for $t + 1$ and $i = i_1$, the lowest value of i in its range. For the rest of the values of i, that is, for $i_j = i_0 + j$ and $2 \le j \le 2^t$, so that $2^t - 1 < i_j \le 2^{t+1} - 2$, Equation (12) gives that $v_2(\binom{n}{i_j+1}) > q - t$. For $j = 2$ from (15),

$$v_2(\alpha_{i_2}) = \min\left(v_2\left(\binom{n}{i_2+1}\right), v_2(\alpha_{i_1})\right) = \min\left(v_2\left(\binom{n}{i_2+1}\right), q - t\right) = q - t.$$

This may be continued for the rest of the values of j, so (14) is true for $t + 1$. □

https://doi.org/10.1017/S1446788712000195 Published online by Cambridge University Press

LEMMA 14. *For n even,* $\mathrm{cont}(E_n) = \mathrm{cont}(R_n) = 2^h$*, where $h = 1$ if n is a pure power of* 2*, and $h = 0$ otherwise.*

PROOF. According to (5), for n even, $R_n = E_n^{A_6}$. Then, from Lemma 7,the content of R_n is the same as that of E_n. From the definition of R_n it suffices to compute the content of $F_n = (x+1)^n + x^n - 1$. Since the coefficient of x^n in F_n is 2, the content must be either 1 or 2. Let $n = 2^q m$ for $q \geq 1$ and $m \geq 1$ odd. Since $(x+1)^{2^q} \equiv x^{2^q} + 1 \bmod 2$, it follows that $F_n \equiv (x^{2^q} + 1)^m + x^{2^q m} - 1 \bmod 2$. When $m > 1$, the coefficient of $x^{2^q} \bmod 2$ is m, which is odd, and therefore $\mathrm{cont}(R_n) = 1$. When $m = 1$ $(n = 2^q)$, $F_n \equiv 0 \bmod 2$, so $\mathrm{cont}(R_n) = 2$. □

THEOREM 15. *R_n, S_n and E_n are irreducible over $\mathbb{Q}$ for $n = 2^q m \geq 4$, where $q =$ 1, 2, 3, 4, 5, and $m \geq 1$ is odd.*

PROOF. Direct computation shows that R_4, R_8, R_{16} and R_{32} are irreducible over $\mathbb{Q}$. Therefore, setting $n = 2^q m \geq 4$, where $q = 1, 2, 3, 4, 5$, it may be assumed that n is not a pure power of 2, that is, $m \geq 3$.

For n even, recall that $R_n = \sum_{i=0}^{n-2} \alpha_i x^i$, where α_i is given by (1). Note that $R_n(0) = \alpha_0 = n$, and from the definition of R_n, $R_n(1) = 2^{n-1}$. According to (4), $R_n = R_n^{A_3}$ so that $R_n(x) = R_n(-x-1)$ and therefore $R_n(-2) = 2^{n-1}$.

Assume that R_n is reducible over $\mathbb{Q}$. Applying Corollary 9 to $f = R_n$ with $A = A_3$, there exist primitive relatively prime polynomials $g_1, g_2 \in \mathbb{Z}[x]$, of degree $r \geq 1$ and $s \geq 1$ respectively, such that $R_n = \lambda g_1 g_2$, where $\lambda \in \mathbb{Z}$ is the content of R_n, with either (1) $g_1(x) = g_1(-x-1)$ and $g_2(x) = g_2(-x-1)$, or (2) $g_1(x) = g_2(-x-1)$ and $g_2(x) = g_1(-x-1)$ (with $r = s$ in case (2)). The signs have been dropped by applying Corollary 5, and since r and s are even, we have $r, s \geq 2$. From Lemma 14, since n is assumed not to be a pure power of 2, set $h = 0$ and $\lambda = 1$.

Put

$$g_1(x) = \sum_{i=0}^{r} a_i x^i \quad \text{and} \quad g_2(x) = \sum_{i=0}^{s} b_i x^i,$$

where $a_i, b_j \in \mathbb{Z}^+$. Identifying coefficients in $R_n = g_1 g_2$ gives $\alpha_i = \sum_{j+k=i} a_j b_k$. Since $\deg R_n = n - 2 = r + s \geq 4$, we have $n \geq 6$. But in case (2), $r + s = 2r = n - 2 = 2(2^{q-1}m - 1)$ so that $r = 2^{q-1}m - 1$, which is odd for $q > 1$. From this contradiction case (2) is impossible for $q > 1$.

Since $a_0 b_0 = \alpha_0 = 2^q m$ with $q \geq 1$, then at least one of a_0, b_0 must be even. In fact both $a_0 = g_1(0)$ and $b_0 = g_2(0)$ are even, as follows. Suppose that one of a_0, b_0 is odd, and the other even. Then one of $g_1(-2)$ or $g_2(-2)$ is odd. In case (1) $g_1(1) = g_1(-2)$ and $g_2(1) = g_2(-2)$, while in case (2) $g_1(1) = g_2(-2)$ and $g_2(1) = g_1(-2)$. Then in both cases one of $g_1(1), g_2(1)$ must be odd, and $R_n(1) = g_1(1)g_2(1) = 2^{n-1}$ so that the odd one of $g_1(1), g_2(1)$ must be equal to 1. But since all of the coefficients of g_1, g_2 are positive, and since their degrees are $r \geq 2$ and $s \geq 2$, it follows that $g_1(1) > 1$ and $g_2(1) > 1$. From this contradiction it follows that both a_0 and b_0 are even. Let $A_i = v_2(a_i)$ and $B_i = v_2(b_i)$ for $i = 0, 1, 2, \ldots,$ so that $a_i = 2^{A_i} M_i$ and $b_i = 2^{B_i} N_i$ where $M_i, N_i \geq 1$ are odd. Then, in particular, $A_0 \geq 1$, $B_0 \geq 1$, $A_0 + B_0 = q$ and $M_0 N_0 = m$.

Since $q = A_0 + B_0 \geq 2$, the assumption that R_n is reducible over $\mathbb{Z}$ must be false for $n = 2m$ ($q = 1$). According to (5) and (6), $R_n = E_n^{A_6}$ and $R_n = S_n^{A_2}$, so it follows from Lemma 7 that E_{2m} and S_{2m} are irreducible over $\mathbb{Q}$.

Since a_0, b_0 are even, $g_1(-2)$ and $g_2(-2)$ are both even, and since $g_1(1)g_2(1) = 2^{n-1} = g_1(-2)g_2(-2)$, put $g_1(-2) = 2^{t_1}$ and $g_2(-2) = 2^{t_2}$, for integers t_1, t_2 where $t_1 \geq 1$, $t_2 \geq 1$ and $t_1 + t_2 = n - 1 \geq 5$. Then,

$$g_1(-2) = 2^{A_0}M_0 - 2a_1 + 4a_2 - \cdots + (-2)^r a_r = 2^{t_1}, \tag{16}$$
$$g_2(-2) = 2^{B_0}N_0 - 2b_1 + 4b_2 - \cdots + (-2)^s b_s = 2^{t_2}, \tag{17}$$

and

$$g_1(-2) = g_1(1) = 2^{A_0}M_0 + a_1 + a_2 + \cdots + a_r = 2^{t_1}, \tag{18}$$
$$g_2(-2) = g_2(1) = 2^{B_0}N_0 + b_1 + b_2 + \cdots + b_s = 2^{t_2}. \tag{19}$$

Since all of the a_i, b_j are at least 1, it follows from (18) and (19) that $2^{t_1} \geq 2^{A_0}M_0 + r$ and $2^{t_2} \geq 2^{B_0}N_0 + s$, where $r \geq 2$ and $s \geq 2$. Therefore $t_1 \geq A_0 + 1$ and $t_2 \geq B_0 + 1$. Note from (14) that

$$v_2(\alpha_0) = q, \quad v_2(\alpha_1) = v_2(\alpha_2) = q - 1, \quad v_2(\alpha_3) = v_2(\alpha_4) = q - 2. \tag{20}$$

Assume that $q = 2$ ($n = 4m$). Since $A_0 + B_0 = q = 2$, we have $A_0 = B_0 = 1$ so $t_1 \geq 2$ and $t_2 \geq 2$. Since $4 | 2^{t_1}$ and $4 | 2^{t_2}$, it follows from (16) and (17) respectively that $M_0 - a_1$ and $N_0 - b_1$ are even, so a_1 and b_1 are odd. Now $\alpha_1 = a_0b_1 + a_1b_0 = 2(M_0b_1 + N_0a_1)$, and since M_0, N_0, a_1, b_1 are odd, $v_2(\alpha_1) \geq 2$. But from (20), $v_2(\alpha_1) = 1$. From this contradiction, R_{4m} is irreducible over $\mathbb{Q}$. Again applying Lemma 7 with (5) and (6), it follows that E_{4m} and S_{4m} are irreducible over $\mathbb{Q}$.

Assume that $q = 3$ ($n = 8m$). Since $A_0 + B_0 = q = 3$, either $A_0 = 1$, $B_0 = 2$, or $A_0 = 2$, $B_0 = 1$. Without loss of generality, assume that $A_0 = 1$ and $B_0 = 2$ so $t_1 \geq 2$ and $t_2 \geq 3$. Then a_1 is odd and b_1 even by (16) and (17), respectively. Put $b_1 = 2b_{11}$. Now

$$\alpha_1 = a_0b_1 + a_1b_0 = 4(M_0b_{11} + N_0a_1),$$

and, since $v_2(\alpha_1) = 2$, $v_2(M_0b_{11} + N_0a_1) = 0$. Therefore $v_2(b_{11}) \geq 1$, that is, b_{11} is even, so $v_2(b_1) \geq 2$. Since $8 | 2^{t_2}$ it follows from (17) that $N_0 - b_{11} + b_2$ must be even, so b_2 is odd. Since $v_2(a_0b_2) = 1$, $v_2(a_1b_1) \geq 2$ and $v_2(a_2b_0) \geq 2$, applying (13) gives

$$v_2(\alpha_2) = v_2(a_0b_2 + a_1b_1 + a_2b_0) = 1.$$

But from (20), $v_2(\alpha_2) = 2$. From this contradiction R_{8m} is irreducible over $\mathbb{Q}$. As previously, applying Lemma 7 with (5) and (6), E_{8m} and S_{8m} are also irreducible over $\mathbb{Q}$.

For the sake of brevity, the detailed proofs of the cases $q = 4$ and $q = 5$ are omitted. They are proved in the same way as the previous cases, by comparing $v_2(\alpha_i) = v_2(\sum_{j+k=i} a_jb_k)$ with the valuation given from (20). Only the possibilities $A_0 + B_0 = q$

need to be considered. For $q = 4$ this means $A_0 = 1$, $B_0 = 3$ and $A_0 = 2$, $B_0 = 2$. The values of α_i for $i = 0, \dots, 3$ are needed to prove $q = 4$ impossible. For $q = 5$ the values of $v_2(\alpha_i)$ for $i = 0, \dots, 4$ are required. It seems likely, but not certain, that the method could be applied successfully to $q > 5$ with the length of proofs growing approximately quadratically with q, as $v_2(\alpha_i)$ is required for $i = 0, \dots, q - 1$, and for each i the number of pairs of values for $A_0 \geq 1$, $B_0 \geq 1$ to be considered is $\lfloor q/2 \rfloor$. $\square$

Acknowledgements

The author would like to thank Dr Keith Matthews and an anonymous referee for helpful suggestions on improving the manuscript.

References

[1] F. Beukers, 'On a sequence of polynomials', *J. Pure Appl. Algebra* **117/118** (1997), 97–103.
[2] A. Cauchy and J. Liouville, 'Rapport sur un mémoire de M. Lamé relatif au dernier théorème de Fermat', *C. R. Acad. Sci. Paris* **9** (1839), 359–363.
[3] C. Helou, 'Cauchy–Mirimanoff polynomials', *C. R. Math. Rep. Acad. Sci. Canada* **19**(2) (1997), 51–57.
[4] B. C. Irick, 'On the irreducibility of the Cauchy–Mirimanoff polynomials', PhD dissertation, University of Tennessee, Knoxville, 2010.
[5] W. Klösgen, 'Untersuchungen über Fermatsche Kongruenzen', Gesellschaft Math. Datenverarbeitung, Nr. 36, Bonn, 1970.
[6] D. Mirimanoff, 'Sur l'équation $(x + 1)^l - x^l - 1 = 0$', *Nouv. Ann. Math.* **3** (1903), 385–397.
[7] P. Ribenboim, *Fermat's Last Theorem for Amateurs* (Springer, New York, 1999).
[8] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, 3rd edn (A. K. Peters, Natick, MA, 2002).
[9] G. Terjanian, 'Sur la loi de réciprocité des puissances l-èmes', *Acta Arith.* **54**(2) (1989), 87–125.
[10] P. Tzermias, 'On Cauchy–Liouville–Mirimanoff polynomials', *Canad. Math. Bull.* **50**(2) (2007), 313–320.

PAUL M. NANNINGA, Centre for Mathematics and its Applications,
Mathematical Sciences Institute, Australian National University,
Canberra, ACT 0200, Australia
e-mail: paul.nanninga@anu.edu.au

https://doi.org/10.1017/S1446788712000195 Published online by Cambridge University Press